Cyber Security

for beginners

Start here

What Cyber Security for Beginners is all about

Welcome to the most practical cyber security course you'll attend!

I'm Andra, and along with the Heimdal Security team, we'll take you on a wild ride in the universe of cyber security. We'll check all the important "sights" - **no fluff, no detours, just the stuff you can really use!**

So I think you'll agree with me when I say:

It's REALLY difficult to try to cut through the noise and get just the information you need when it comes to cyber security.

We know there's waaay too much stuff online about the subject, from really technical articles to big data breaches suffered by Forbes Top 100 companies.

***"So how can I find relevant, actionable advice?"*, you may ask**

I believe in curated content and its power to **SAVE you TIME and EFFORT** by providing the right insights at the right moment.

So here's what I want to do for you: provide a guide to help you increase the security of your digital assets with **as little hassle as possible!**

Now it's time to kick things off with an overview of the **action-packed lessons** you'll explore in this course:

***Long list?* Not to worry!**

Your time will be well spent and I promise that we'll do our best to make this course fit your needs and expectations.

Anyone, anywhere, anytime can become a victim of cyber hacking (including you), but there's a lot you can do to increase your chances of not getting hacked. And I'm here to help you become a **Cyber Security Ninja!**

As a Cyber Security Ninja, will I have 100%, bulletproof, state of the art security by the end of the course?

We're not afraid to say this: the answer is NO.

Any security expert will agree that **there is no such thing as impenetrable cyber security**, simply because things constantly change.

But people who stay safe online do one thing very well:

They take the time to create a system that protects them, which, once put in place, doesn't require much time to maintain or upgrade every now and then.

The secret to keeping your data safe from cyber criminals is to not only read the material in this course, but also ACT on it.

So here is my first BONUS for you (more will come along the way) and your first actionable item:

Start **by assessing your personal information security level** by using **this quick checklist**.

You can download it, complete it and see what things you could still improve. And be sure to keep it to see how much progress you'll make by the end of the course.

Like I said, this course will be as hands-on as possible, so **ACTION IS KEY** to dramatically improving your safety and your data's safety online!

If you have any questions along the way or need extra information, please feel free to contact me at any moment at **aza@heimdalsecurity.com** and I'll get back you in 24 hours at most.

Lesson 1 /19

Security 101: cover your basics in less than 1 hour

Lesson 1

Before I start this lesson, let me tell you that me and the Heimdal Security team will be next to you along the way in this cyber security course and we'll discover together the online security information which will improve your Internet safety knowledge.

And since I want to keep this content easy to understand and apply, I will try to "translate" the technical cyber security terms along the way in a language that we can both relate to.

Since this is the first actual lesson, my immediate priority is to make sure your system is protected **right now**.

To accomplish this, I organized an **actionable guide** in **11 simple** steps that you can follow to greatly improve your security FAST!

11 Steps to Improve Your Computer Security in Less Than 1 Hour

1. Use strong passwords for your email and social media accounts

There are a few things you need to pay attention to when dealing with setting good passwords for your online accounts. First of all, **don't use the same password in more than one online account!**

The reason is quite easy to guess: if one of your online accounts is hacked, then the others will soon follow. By using different passwords, you reduce the potential loss you could suffer in case this privacy breach takes place.

One of the best ways to ensure your online accounts are not accessed by anyone else but you is to use the 2 step verification method. Activating this method means that you will have to enter, besides your credentials, a code sent to your phone. Using this method, you can protect your private information from social media accounts or important data from your email account.

We have a step-by-step guide dedicated to password management, coming up in **lesson 4**!

2. Stay safe from spyware threats with a specialized security solution

First, let's establish fast, *what exactly is spyware?* Spyware refers to software which is capable of installing on your computer and starts opening pop-up windows, redirects your browser to malicious websites and monitors your browsing sessions affecting your private Internet connections. (You'll figure out all this semi-technical gibberish in lesson 3, I promise!)
There are a few signs which should trigger a sign of alarm:

- computer is slow when opening programs or running some applications
- pop-up windows appear all the time
- a new toolbar may appear in your web browser
- the Home page of your web browser has been modified
- the search engine in your web browser has been changed
- error messages start to appear unexpectedly

To stay safe from spyware, use one of the popular anti-spyware products available online. A few security solutions capable of removing spyware from your system are Malwarebytes, Spybot Search and Destroy, Lavasoft's Ad-Aware, etc.

At the same time, simply follow these good security practices:

- Don't click any suspicious links or pop-up windows
- Don't answer to unexpected answers or simply choose No
- Be careful when downloading free applications

3. Keep your Windows operating system and your vulnerable applications up to date

I am quite sure you read lately many security news regarding software vulnerabilities and you ask yourself: ***what can I do?***

Many people don't take this news seriously, since most security solutions are mainly created for malicious software.

But software vulnerabilities are not something you can ignore. Taking advantage of software vulnerabilities present in popular programs and applications is a popular method used by online criminals.

So, if you know you use popular software, like Java, Adobe Flash, Adobe Shockwave, Adobe Acrobat Reader, Quicktime or popular web browsers like Chrome, Mozilla Firefox or Internet Explorer, always make sure you have the latest available patches.

You need to understand that these software solutions are always under threat from criminal minds, so don't rely on your memory and install a dedicated solution to perform these actions for you.

4. Use a standard user account in your Windows operating system to go online

Different levels of rights and privileges are available for the Windows user accounts. I recommend using a standard Windows user account to access Internet.

If you use a standard account in your Windows operating system, you make sure that a piece of malware which could infect your limited user account will not be capable of doing great damage to your system.

Only an administrator account can make significant changes to your system, like deleting important Windows related files or installing malicious software. If you use your standard account, you will have to provide the credentials for the administrator account every time you make an important change.

5. Don't turn OFF your UAC (User Account Control)

I must admit, this is something I also have the tendency to do:

Turn the UAC off as soon as I install/reinstall my Windows operating system.

But should I do it? Does this make my system more secure?
The answer is **No**.
What if, instead of completely turning it off, maybe you can only decrease the level of protection by using the provided slider?

The role of UAC is to monitor what changes occur on the system and when an important event takes place, like installing or removing an application.

The UAC makes sure you have administrator permissions and that you really want to take that action. In case your Windows user account has been infected, UAC helps you by keeping suspicious software from making changes on the system.

6. Go online with a secure browser

Your web browser is the main tool you use to access Internet and you should pay a great deal of attention to secure it correctly. At the same time, vulnerabilities from web browsers are like open invitations to hackers. By using these open doors, online criminals attempt to retrieve private data from your system.

To **secure your online privacy**, you can follow these recommendations:

- Choose the latest version for your browser and make sure you have the latest security patches installed. This is important and keeps your system secure from online criminals' attacks.

- Increase your privacy and security settings in your browser. Epic, user-friendly how to's coming up in **lesson 10**!

- Choose a private browsing session when you access a website you are not sure about. Choosing this navigation mode will prevent your browsing session details from being stored.

- Use secure websites for sensitive financial operations. To visit a secure website, make sure the web address starts with “**https://**”. The “**s**” comes from “**secure socket layer**“, and it indicates you are connected to a website where data, which is sent and received, is encrypted.

7. Don’t trust public and free Wi-fi networks

Be careful when connecting to public and free wireless networks. One of the favorite methods used by online criminals to retrieve your credentials is by using wireless sniffers to access data sent over unprotected networks.

One way to increase your security is by using a “private browsing” session, this way you make sure your credentials won’t be stored locally. Nevertheless, this won’t stop the Internet Service Provider or anyone else “listening” out there to catch your private communication.

With the increasing danger of online theft and lack of privacy on popular social platforms, such as Facebook, you need to safeguard your freedom and protect your Internet activities. One way of keeping your browsing session private and secure is to use a VPN (that is a Virtual Private Network).

Getting your home Wi-Fi and devices in tip top shape for online browsing is what **lesson 11** is all about. Cyber criminals won't know what stopped them!

8. Check the link before you click it

Phishing threats are usually done by using email messages that apparently come from financial institutions or well-known banking websites. These attempts to retrieve private information from a user provide links in the message that direct the victim to a fake web location, controlled by online criminals.

To make sure you won't be infected by clicking on dangerous links, hover the mouse over the link to see if you are directed to a legitimate location. If you were supposed to reach your online banking website, but the link indicates "hfieo88.net", then you should not click the link.

So, how can I know where I'll end up if I click it?

To make sure you are going to the right direction, use a free tool such as Redirect Detective. This tool will allow you to see the complete path of a redirected link. Another tool which can provide very helpful in checking suspicious links is the reliable URL checker, **VirusTotal**: **https://virustotal.com/**.

9. Don’t forget to log out

Don’t simply close your browser when you are done with your financial operation or when you exit your online account.

You need to remember that you have to log out from your online account. If you don’t do this, especially if you are in a public location, the next person who opens the Facebook account, for example, will access directly your Facebook profile.

I recommend you using a virtual browser for your financial operations to keep your online banking secure. Private browsing sessions are also recommended if you want to prevent authentication credentials (or cookies) from being stored.

10. Don’t post private information on your social media accounts

Exposing personal details may lead hackers into finding your financial information. For the same reason, check your kids’ social media behavior to make sure they won’t expose private information that may possibly be used against you, in phishing attacks.

Lesson number 13 is packed with ready-to-use advice on how to stay safe while using social media.

11. Don't access questionable web locations

Don't access or download content from unknown or controversial locations. Access websites that proved to be safe and you know you can trust.

Nevertheless, this is not a guarantee that you won't get infected. Nowadays, cyber-criminals exploit vulnerabilities in legitimate websites and inject malicious code, as to perform drive-by attacks on unsuspecting visitors.

It may be a free screen saver or a browser toolbar that may infect you with a keylogger (definition coming up in **lesson 3**!) that can record and send your personal data to cyber-criminals.

To make sure your system is protected and your credentials are not exposed, install a security product, which can detect and stop hackers from stealing valuable information from your system.

Thanks for sticking with us until the end!

We tried to cover the minimum steps that can be taken in a short period of time to greatly increase a system's security.

Though you may not have the time right now to follow them all, just remember you can always go back to this paper when you feel the need to go over the info again.

Lesson 2 /19

The 10 Internet Security Myths You Need to Forget

Lesson 2

The previous lesson covered the minimum steps you need to take to stay safe online.

Now, I know there is a lot of conflicting information out there, which creates controversy, but these stories or “myths” are now part of Internet culture and it’s difficult to separate fact from fiction, especially when so many people treat them as “real”.

Since it is a confusing topic that covers so many areas on the web, it is difficult to see beyond half-truths or falsehoods. The information and data in the online world shifts and covers new interests, therefore our security perspective must also keep up and separate fact from fiction.

Here are the top **10 most common security myths** that need to be demolished, before you take any security action on our systems.

10 Internet Security Myths That You Need To Forget

1. This can’t happen to me, only important or rich people are targeted.

This security myth is called by many security experts **security through obscurity.**

Simply said, the Internet is such a big place that no one wants to target **you**. And even if someone would try to attack your system, there wouldn’t be too much valuable data to be stolen.

In most cases, the user who embraces this kind of thinking doesn't actually want to lose time or money to address this security issue for the system.

The problem with this type of wishful thinking is that **it doesn't take long until an IT criminal disables your system by using one of your system's vulnerabilities.**

This happens because it is not about how you are, it's only about your system protection level.

Using automated tools, online criminals probe systems to discover vulnerable computers and networks to take advantage of.

And it's not just about your personal information they are after: your Internet-connected system is also a valuable asset they can use for their malicious actions.

Even if you think there is no important personal or financial data on the system, a potential identity theft or IT criminal can still use the little data discovered and relate it to other information taken from other sources in order to have a complete picture.
Why take a risk when there are so many protection products and even free tools to keep you safe from malware?

So, don't trust the odds that tell you that you should be safe out there.

2. Install this security application and you'll be fine.

This security myth is also called **the search for the magic bullet that can solve all your system security.**

A user that pays for a security program has high expectations and hopes all his system security to be covered by just installing the purchased program. This myth represents a false image of what it means to have a complete system security.

Trusting one security program to cover your system, your online actions, keep you safe against data and financial stealing malware and other non-traditional attack vectors means that you place too much trust in a single line of defense.

To have an antivirus software or any other security program doesn't mean to cover the whole Internet security front, though there are some antivirus products that try to create the impression that everything is protected by just installing that single program.

To have complete protection of your system and your online actions, you should start by using an antivirus program that protects you against classical threats, such as viruses, worms, Trojans or phishing. At the same time, you also need solutions against spam, data and financial stealing malware, a parental control tool and a good firewall.

More than anything, you need to stay up to date with security and the latest news and **reject false stories that promise total protection by installing a single security program.**

Because cyber criminal attacks are evolving faster than antivirus can, next-generation anti-hacking tools have emerged! And I'll tell you all about them in **lesson 6**.

3. I don't need security programs because I don't access unsafe locations.

I'm sure you heard about this one and you have those friends that believe simple common sense is all that is necessary to keep you safe from malware, viruses, spam, phishing, identity theft, online attacks, etc.

How many times have you heard someone saying: *I don't need antivirus protection, I'm too smart to fall for those* *tricks!*

And if it's about email attachments, risky web locations or pop-up ads, that may be correct.

But is that all?
What about malware attacks and vulnerability checks that are not easy to detect?
Or about malicious code hidden in legitimate websites?

To be safe online is quite similar to driving your car.

You may have common sense and pay attention to potential dangers, ***but can you always predict what others are doing around you in traffic?***

Now, you **understand** why security is important.

4. I set some strong and complex passwords to my accounts, so I'll be OK.

It is a common recommendation for every user to set a strong password. Your passwords should have 10 or 20 characters and they must contain various letters and numbers. Making the password long and complicated is supposed to create serious difficulties for someone that tries to break it.

These complex passwords that are set nevertheless present a major inconvenience: they are quite difficult to remember and you are forced to write them down in the PC or on some piece of paper, which increases the risk of unauthorized access to the account or to the operating system. At the same time, users have a tendency to dislike such a strong password implementation and start to perceive this as a burden.

Normally, most Internet users set quite easy to remember passwords to their accounts or they use passwords which are easy to guess.

Therefore, **most passwords and credentials, which are even used for online banking locations, are actually sniffed and not so much cracked.** Another well-known fact is that users set the same password for different online accounts, which makes the job much easier for an online criminal.

The need for a good password is part of a larger security scheme that includes security programs for classical and non-traditional vector attacks, spam detection and phishing attempts.
But fancy words won't keep you safe. ACTIONS will! Password management and security is the star of **lesson number 4.**

5. Internet security is expensive.

I'm sure you spend some time online, running various activities, sending messages to friends on social media accounts, purchase various items on different websites, not to mention accessing your banking account to send and receive money.

So, is Internet access just a simple way of wasting time and having fun, or is it an integral part of our lives?

How difficult is it for an IT criminal to use information from our Facebook account and correlate it with data obtained from malicious software already installed on our system in order to have a complete image of your life?

And, from that point, ***how long until your identity is stolen and used for malicious purposes?***

I am sure you heard about cases when someone's online identity has been stolen and money removed from the banking account. What you don't hear is that recovering from this online attack takes time, even years and since an attack can occur from any part of the world, the perpetrators are rarely brought to justice.

With this information in mind, should you still take a chance online?

It is true you could install free antivirus on your system and there are many options online, but from my experience I recommend using a good security product from a big company name.

To choose the best solution, access the antivirus test results run by established names in the security industry, such as **AV Comparatives**, **PC Magazine**, **AV-TEST** or **Virus Bulletin** and select the best security solution for your system.

6. I only open emails from my friends, so I should be fine.

How many of us already received a strange email from a friend or from a relative?

How difficult is it to spoof an email in order to display anyone's name as being the sender?

If you are used to these types of tricks, you may be safe from clicking the links contained in the email or download on your system the attachments of the email.
But for someone who is less skilled in Internet security, **just one click away from malicious software can get them infected.**

Clicking a link may send the user to a malicious website controlled by online criminals and downloading the content of the email may easily install on the system some dangerous financial stealing malware, which remains hidden stealing banking credentials for cyber-criminals.

These types of emails may also appear like coming from financial institutions and they can look **real** enough to trick you into giving away private information from your online account.

In this case, if you have doubts about the origin of the email, **simply contact directly the institution or your friend and ask if they sent that particular email.**

Email is part of our lives just like our phone agenda, so I'll teach you how to keep cyber criminals out of your inbox in **lesson 12**.

7. I download and access information from trusted sources. This keeps me safe.

This is a pretty difficult security myth to break. Most of us think that accessing **safe** and **secure** locations will keep us safe.

The reality is quite different. Even if you access a trusted source, you are still vulnerable to online dangers, and I'm not referring just to old viruses, worms or other **normal** malware.

In this particular case, I'm talking about a much greater danger: malicious software developed by cyber-criminals that target our private data and financial credentials, and which is designed to remain hidden from classical antivirus detection.

This type of malware usually spreads through emails that apparently come from a secure financial institution (or from a friend), through drive-by downloads, malicious content placed on secure websites that download on your system, or simply through pop-up ads placed by online criminals on those websites that are considered safe to access.

To stay safe from this danger, you need an especially designed software to protect you against financial theft and data stealing software. This type of software offers a complementary layer of security which the normal antivirus products cannot provide. Don't worry, I'll tell you all about it when time comes.

8. My social networks are safe places. Friends will be friends.

But will they? Social media services, such as Facebook or Twitter, brought so many people online in the last years that it is difficult to find someone who doesn't have at least a single online account, at least LinkedIn (which is focused mainly on jobs, but has recently started to develop into a more interactive network).

And since so many people are connected this way, online criminals have already developed tricks and methods that target these networks, especially with online scams and identity theft attempts. For a complete list on online scams, you can take a look on this article.

If online criminals can place malicious content like drive-by downloads and pop-up ads on safe websites, **they can do the same with social media accounts.**

Who doesn't have that friend in the list that clicked an offer on a fake page spreading it after to the entire list of friends?

Another danger found on these types of social media accounts is posed by online criminals that create fake profiles and personas to retrieve personal information from other users.

By collecting information (that doesn't seem very important initially) and connecting it to other data retrieved from other locations, **the IT criminals can track online habits and build a user persona in order to operate the identity theft of the targeted user.**

Therefore, be careful who you add to your list of friends.

And remember that **lesson 13** will feature need-to-know (and especially **need-to-APPLY**) tips about social networking – the safe way.

9. I don't have important information or sensitive data on my system. Why should I worry?

First of all, *are you sure there is nothing valuable on your system?*

Did you let your browser remember all your passwords for your online accounts, banking websites and your email address?

How much damage can you take if your email account is accessed?

You may think that your data is not important for a cyber-criminal, but you should know they can collect and assemble information about you from other sources as well to have a big picture of your online habits. Later on, they can use the information to steal your online identity and use it against you.

And even when there is no important data for a potential criminal on your system, they still can use your device for various purposes.

They can use your system's hard disk to store illegal content, install a bot to use your computer in a coordinated online attack, host phishing content or share criminal materials. At the same time, they can use your system's resources, such as your Internet connection to access remote websites or your email address to send spam to your list of friends.

Are you worried now?

10. In case I get infected, I will see that for sure.

Well, don't be so sure about this.

In the past, when a computer started running slow and pop-ups appeared all over the screen, maybe you could tell. But **today, cyber-criminal methods have evolved and increased their efficiency** that in most cases, a normal user can't tell his system is involved in spam campaigns or coordinated online attacks.

The malicious software is built to be undetectable and untraceable by antivirus products, retrieving private information without you even noticing. Designed to evade normal detection systems and working in the background, the latest data stealing malware retrieves private data like credit card details and account logins without leaving visual evidence.

But fear not! For I have designed **lesson 16** to help you detect and block malicious attempts to hack and control your device!

We tried to cover the main security myths that exist in the online world, stories that actually appeared because we try to find easy solutions and simple answers to our security fears.

Though you may not have the time right now to discover them all, just remember you can always go back to this lesson when you feel the need to go over the info again.

Lesson 3 /19

No more technical gibberish! Master basic security terms in 20 minutes

Lesson 3

Hi there,

In the last lesson, we talked about 10 Internet security myths that are worth tossing to trash.

Now that we got that mess out of the way, we're about to dive into the "meat" of the course, and I plan to share **insider knowledge** with you throughout the next lessons.

From my experience, when reading about cyber security, 2 things can happen:

1. You can either become **fascinated** with the subject and make it a bit of a (necessary) hobby...

2. Or you can be put off by the technical lingo you don't understand and just drop the whole thing.

Learn to speak "cyber security" in less than 20 minutes!

In the time it would take you to eat 4 sandwiches (depending on how big the sandwich really is), you can learn **18 essential information security terms** and gain the basic knowledge you need.

And you'll acquire one more skill: understanding how cyber criminals think and act! Get inside the mind of the enemy, so you can beat them at their own game.

So let's get to it:

Lesson 3

18 essential cyber security terms you REALLY need to know

1. Antispyware Software

Anti-spyware software is used in detecting, blocking and/or removing spyware attempts.
Spyware is a type of software that seeks to gather your personal information, without your permission. It has the capability to take over your computer entirely! The information it collects is then sent to a third party without your consent.

There 4 main different types of spyware:

- system monitors,
- Trojans,
- adware,
- and tracking cookies.

Spyware is mainly used for tracking a user's movements online and serving annoying and dangerous pop-up ads.

HOW YOU CAN GET INFECTED:

Your system can get infected with spyware if you visit certain websites, by pop-up messages that ask you to download an application or program (told you they're evil!), through security holes in the browser or in other software, etc.

Usually, spyware is well hidden and it's also difficult to observe. You might notice a spyware infection when the virus starts using your system's resources and slows it down in a way that'll make you really, really angry.

2. Antivirus Software

Antivirus software, sometimes called an anti-malware program (you can also call it AV if you want to show off), is computer software used to prevent, detect and remove malicious software.

Antivirus protects your computer from a large number of threats, such as ransomware, rootkits, Trojans, spyware, phishing attacks or botnets.

Without getting technical, let's just say that the way antivirus scans for infections is not really coping with current threats. Cyber criminals are smart. Really, really smart! And their attacks are vicious, so just remember that **anti-virus is not enough** and you need something more to keep you safe.

But that doesn't mean you don't need antivirus. YOU DO, trust me! But you need other stuff too and I'll tell you more about that later on.

software, etc.

Usually, spyware is well hidden and it's also difficult to observe. You might notice a spyware infection when the virus starts using your system's resources and slows it down in a way that'll make you really, really angry.

3. Cyber-Attack

A cyber-attack is classified as any type of offensive action used by cyber criminals to deploy malicious code in your system with the purpose of stealing, altering, destroying or taking any advantage from this action.

Cyber-attacks can target both people and things. ANYWHERE. ANYTIME. Individual users, computer networks, information systems, IT infrastructure of all types and sizes – no one is safe! (And I'm not being dramatic about it.)

And smarter cyber criminals launch stronger attacks, which lead to worse consequences.

4. Drive-by download

A drive-by download can refer to 2 things:

a. A download which you authorized but without understanding the consequences (example: downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).

b. The unintentional download of a virus or malicious software (malware) onto your computer or mobile device.

HOW YOU CAN GET INFECTED:

Drive-by downloads can happen when you visit a website, when reading an email or by clicking on a deceptive pop-up window.

These type of malicious downloads usually take advantage of (or "exploit") a browser, an app, or an operating system that is out of date and has a security flaw that has not been solved or patched.

This is why **it's crucial to constantly maintain your software updated.** (No worries, I'll nag you about this along the way.)

5. Exploit

An exploit is a piece of software, a chunk of data, or a set of commands that takes advantage of a bug, glitch or vulnerability in order for malicious purposes.

Exploits can cause disruptions in the behavior of computer software, hardware, or something electronic (usually computerized).

HOW YOU CAN GET INFECTED:

By using exploits, **cyber criminals can gain control of your computer.**

After that, they can do pretty much what they want.

One of the ways to protect yourself from exploits is to **keep your software updated at all times** (told you I'd nag you about this!) and take all essential security measures (which I'll show you in this course).

6. Keylogging

Keylogging (also called keystroke logging) is a method that cyber criminals use to record (or log) the keys you strike on your keyboard in order to get confidential information about you.

Of course they do this in a concealed manner, so that you won't know you are being monitored while typing passwords, addresses and other secret data on your keyboard as usual.

HOW YOU CAN GET INFECTED:

Keyloggers are usually used with malicious intentions, to steal passwords or credit card information.

Although many anti-spyware applications can detect some software based keyloggers and quarantine, disable or cleanse them, there is no solution that can claim to be 100% effective against this type of threat.

7. Malvertising

Malvertising (short for "malicious advertising") is the use of online advertising to spread malware.
Cyber criminals inject malicious or malware-loaded code into online advertising networks or legitimate websites, which then infect your systems through clicking, redirection or drive-by downloads.

Since online ads are managed by online advertising networks, even a legitimate website may host an infected web banner, although the website itself remains uncompromised. Some of the websites that have unknowingly hosted malvertising are The New York Times, the London Stock Exchange, Spotify, and The Onion.

HOW YOU CAN GET INFECTED:

Cyber criminals use pop-up ads, drive-by downloads, web widgets, hidden iframes, malicious banners, and third-party applications (example: forums, help desks, customer relationship management systems, etc.) to deliver malware. This is why malvertising is so wide-spread, affecting many users without their knowledge.

8. Malware

Malware (short for malicious software) is one of the terms you'll hear most often when it comes to cyber security threats. The terms defines any software used by cyber criminals to:

- disrupt computer operations,
- gather sensitive information,
- or unlawfully gain access to private computer systems.

Malware is characterized by its malicious intent, because it acts stealthily to steal your information or to spy on your computer for a long time, without your knowledge.

'Malware' is a general term used to refer to an entire category of malicious or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other harmful programs.

Lesson 3

HOW YOU CAN GET INFECTED:

Malware is usually spread through executable code, scripts, active content, and other software. The major threat is poses comes from malware being disguised as, or embedded in, non-malicious files, such as .jpeg, .mpeg, .exe, .gif, .mp3 and many, many more.

You should definitely check out this list of **50+ File Extensions That Are Potentially Dangerous on Windows** to get an even better idea of how malware can sneak into your system.

9. Patching

Patching is the process of updating software to a different, newer version. A patch is a small update released by a software manufacturer to fix bugs in existing programs.

A patch can relate to features and usability, but is can also include security features.

Patching is essential for your online security, because it prevents cyber criminals from launching attacks using **Zero Day viruses** (definition at #18).

10. Phishing

Phishing is (yet) another method that cyber criminals use in order to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by posing as a trustworthy entity in emails or other means of electronic communication.

Phishing is an example of **social engineering** techniques (definition at #12) used to deceive users, and exploits the poor usability aspects of current web security technologies.

> **HOW YOU CAN GET INFECTED:**
>
> A phishing email could seem that it legitimately comes from your bank, and could trick you into entering valid credentials on a fake website.
>
> Phishing is done through emails, instant messaging apps or social media posts (on Facebook, Twitter, LinkedIn, etc.).

11. Ransomware

Ransomware is a form of **malware** that essentially holds a computer system captive while demanding a ransom.

This type of malware locks you out of your computer by either:

- encrypting files on the hard drive
- or locking down the system and displaying messages that extort you into paying the malware creator to remove the restrictions and regain access to their computer, usually via a key. The bad news is that the malware creator is the only one who knows the key.

HOW YOU CAN GET INFECTED:

Ransomware typically spreads like a normal computer worm (by replicating itself in order to spread to other computers), and it could infect your system via a downloaded file or through some other vulnerability in a network service.

The chances of retrieving your data are very slim, unless you're willing to pay the ransom (which is why it's crucial to have a back-up of your data in a secure location).

The malware creator will either supply a program which can decrypt the files, or he will send an unlock code that decrypts your data. But there is **no guarantee** that this will happen, even if you pay the requested ransom.

Lesson 3

12. Social engineering

Social engineering is one of the most commonly used methods of cyber hacking, which requires little to no technology. It relies on psychological manipulation to persuade the victims to perform certain actions or divulge confidential information.

HOW YOU CAN BE COMPROMISED:

In this case, cyber criminals use lies, impersonation, tricks, bribes, blackmail, and threats (just like your ex) to attack information systems. Phishing (defined at #10) is also a form of social engineering.

For example, cyber criminals may pose as contractors, exterminators, fire marshals and technicians to go unnoticed as they steal your secrets or trick you into divulging confidential information about your company.

13. Spam

We all know that spam is made of those pesky, unsolicited emails that clog our inboxes. But, in recent years, spam has spread to instant messaging apps, texting, blogs, forums, search engines, file sharing and social media.

HOW YOU CAN GET INFECTED:

While spam itself may not seem very dangerous, it sometimes carries malware, spreads viruses, worms and other types of threats, such as financial theft, identity theft, data and intellectual property theft, fraud, and deceptive marketing.

14. Trojan (Trojan horse)

A Trojan horse (commonly known as a Trojan) is a type of malware that conceals itself as a normal file or program to trick you into downloading and installing malware.

A Trojan can do many dangerous things to your system, like give cyber criminals unauthorized, remote access to your infected computer.

Once that happens, cyber criminals can:

- steal data (logins, financial data, even electronic money),
- install more malware, modify files,
- monitor your activity (screen watching, keylogging, etc.),
- use the computer in botnets (a collection of Internet-connected programs communicating with other similar programs in order to spread malware),
- encrypt your files, like in the case of **ransomware** (defined at #11)

- crash your computer
- format your disks, destroying all the contents on your device, etc.

HOW YOU CAN GET INFECTED:

There are plenty of ways in which your system can become compromised by a Trojan:

- through email attachments
- software or music downloads
- unsafe instant messages
- peer 2 peer downloads
- routine forms that need to be filled in
- drive-by downloads, etc.

15. URL or web content filtering

URL or web filtering technology is software which keeps you from accessing inappropriate websites or content or that prevents you from ending up in a dangerous web location (and by dangerous I mean malware-laden).

The software's filter checks the origin or content of a web page against a set of rules provided by company or person who has installed the URL filter. If the web page has been blacklisted or marked as infected, it will deny access to that web location, blocking a potential cyber attack.

Lesson 3

16. Virus (Computer Virus)

A computer virus (shortly called virus) is a type of malware *(told you it would come up often!)* capable of replicating itself and spreading to other computers and data files.

Viruses spread to other computers by attaching themselves to various programs and executing code when you launch one of those infected programs.

But they're really sneaky, so they can also spread through script files, documents, and cross-site scripting **vulnerabilities** in web apps (defined at #17).

Viruses are also evil, because they can be used to steal information, harm your computers, log keystrokes (**keylogging** – defined at #6), create botnets, spam your contacts, steal your money, display political or humorous messages on your screen (the least of your worries), and more.

(Nasty stuff, I know!)

HOW YOU CAN GET INFECTED:

Viruses install themselves without your consent, because cyber criminals use **social engineering** (defined at #12) and exploit software bugs and **vulnerabilities** (defined at #17) to gain access to your computing resources.

Viruses can reside in executable files (.exe or .com files), in data files (Microsoft Word documents or PDFs), or in the boot sector of your hard drive. Or in a combination of all of these.
And the worst part is that some viruses are polymorphic, which means that the virus has no parts which remain identical between infections, making it very difficult to detect directly with an antivirus solution.

17. Vulnerability

A cyber security vulnerability is a weakness which allows an attacker to undermine your system's data security defenses.

A vulnerability appears at the intersection of 3 elements:

1. **a system susceptibility or flaw** (example: your Java software hasn't been updated to the latest version – *seems pretty innocent, right?*)

2. **attacker access to the flaw** (example: you click on a mal-

ware-infected banner ad which delivers a download on your computer)

3. **and attacker capability to exploit the flaw** (example: now the cyber criminal has a way in, through that malicious download).

A vulnerability is just a pretense that a cyber criminal can use to launch a full scale attack on your system. He still needs the right tools for that, but they come in a large supply online and they're cheap as well.

The way to protect yourself against vulnerabilities is to maintain your software updated at all times, and there are other tips & tricks I'll share in the coming lessons as well.

18. Zero-Day virus

Now that you know what a vulnerability is, it'll be really easy to understand what a Zero-Day virus is as well.

Zero-Day viruses appear when cyber criminals discover a flaw in a piece of software (for example, in Adobe Air). They exploit that vulnerability, launching an attack that users can't defend themselves against, for two simple reasons:

- The flaw they exploit is attacked by launching a previously unknown computer virus or other malware

- Antivi rus programs rely upon signatures to identify malware, but the signature for this new breed of malware or virus is not in their database, because it's new and hasn't been sampled.

  That is why antivirus software is not effective against Zero-Day viruses, and that why you need additional solutions to protect you from advanced attacks such as these.

HOW YOU CAN GET INFECTED:

The usual methods described beforehand work in this case as well:

- drive-by downloads
- malvertising
- spam
- through email attachments
- software or music downloads
- unsafe instant messages
- peer 2 peer downloads
- routine forms that need to be filled in, etc.

The difference is that, once you get infected, there's very little you'll be able to do to stop the infection and mitigate its effects.

But I promise that we will teach you how to strike back against such attacks and keep safe online at all times!

Kudos for sticking with me until the end!

I know it's a lot to take in at once, but remember you can always keep this course and go back to it when you need to.

Lesson 4 /19

Cyber criminals can steal your credentials in 2 minutes. Here’s how to master your password security

Lesson 4

Hey there,

I'd like to start this lesson with one simple question I'd like you to answer (to yourself) honestly:

Have you ever used the same password for more than one of your accounts?

I know that, for most of us (if not for all of us), the answer is a shameful... **YES**.

I've done it too, because, if you think about it, **we've never received a proper education for using the Internet.**

We wouldn't let kids walk around without proper road safety education and we wouldn't let drivers hit the road without knowing the rules.

So why is it that we think that we can go online and put our entire lives there (personal AND professional) ***without being aware of the dangers?***

This lesson is a staple in your education about cyber security.

And the lead character is that string of characters that shield our most prized information:

The mighty PASSWORD!

The problem is that the passwords we use are not that mighty. In fact, we should just admit they're actually LOUSY.

Lesson 4

Putting "12345678" between you and a sophisticated cyber criminal is CRAZY, don't you think?

So it's time you admit your sins and do something about them!

The 7 Deadly Sins of Password Management

1. **You shall not keep your passwords in a text file, spreadsheet, plain text or a similar, unprotected document!**

   Why? Because that flimsy file might get stolen, corrupted, deleted or, worse, retrieved by cyber criminals. I wouldn't like to see you scramble to change 200 passwords as soon as possible if you ever got hacked.

2. **You shall not use the default password sent to you by a service provider!**

   Why? It's simple: because those passwords are usually simple and, consequently, easily breakable. It would be like giving candy to a baby, like they say. And cyber criminals love both your passwords and (probably) candy.

3. **You shall not use one of the shamefully weak passwords listed in this top 10!**

123456
123456789
1234
Password
12345
12345678
Admin
123
111111
1234567

Why? I think the passwords above are self-explanatory, *don't you*?

4. **You shall not use words that can be found in a dictionary or that are common phrases!**

Why? Because cyber criminals have a method called "dictionary attack".

A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the name). And dictionary attacks often succeed, exactly because many people use short passwords that include ordinary words or simple variants obtained, for example, by adding a digit or punctuation character.

5. **You shall not use passwords that include your birth date or other information that's easily available online!**

   Why? Because tracking down your personal information online is what gives cyber criminals a field day. Even if you have your privacy settings pushed to the max, there's always a way around them for a guy that hacks confidential information for a living.

6. **You shall not use the same password without changing it for a long period of time!**

   Why? Because passwords, just like the ice-cream in your fridge, have an expiration date. An old password may be easy to crack and there's a lot that can go downhill from there. Keeping things fresh can keep trouble off your track.

7. **You shall not use the same password twice! This is a big one. Seriously!**

   Why? This is one of the CAPITAL mistakes we all make when it comes to password management. Using the same password for more than one account (and usually making it an easy one) means that cyber criminals will get access to MORE accounts at once, and they'll be able to steal MORE data and do MORE damage!

Imagine if they cracked the password to your online banking account. And that password would be used for your email account as well. **Can you envision the impact** of an attack on your personal finances, and on your professional and personal life?

If that thought made you shudder, let's see what you can do about it.

Here's how cyber criminals try to break your passwords

This is a very quick run through the methods that cyber criminals use to break your passwords and get access to your private information:

- **Phishing** – defined in lesson #3
- **Keylogging** – defined in lesson #3
- **Social engineering** – defined in lesson #3
- **Malware-based attacks** – defined in lesson #3
- **Brute-force attacks** – cyber criminals systematically check all possible keys or passwords until they find the right one. For this, they use algorithms that can try all of these combinations superfast. Your short, repetitive passwords are no match for them!
- **Database hacking** – if a cyber criminal gains access to a company's user database that contains the credentials of

thousands or millions of customers, and you're among one of those customers, then you could be exposed as well. Tenths of attacks such as these have made the headlines in the past 2 years, and they just seem to keep on coming.

So now **let's get to THE FUN PART**, where you get to do a spring cleaning type of thing and change your passwords while going through you accounts.

How to create a good password in 4 easy steps

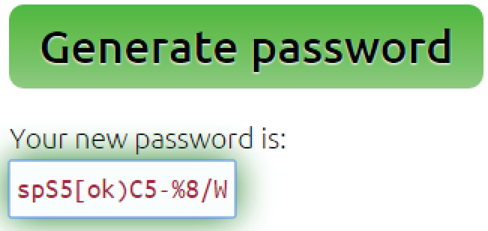
Step 1. **Use a password generator to create long, complex passwords.**

You can use some of the options listed here or come up with one yourself. Just make sure to follow step 2.

Recommended password generators:
https://www.random.org/passwords/
https://identitysafe.norton.com/password-generator/
http://strongpasswordgenerator.com/
http://freepasswordgenerator.com/

Step 2. **Make sure to use a combination of words, numbers, symbols, and both upper- and lower-case letters,** without using adjacent keyboard combinations (such as "qwerty" or “12345678”).

Example of a strong password:



Your new password is:

spS5[ok)C5-%8/W

Step 3. Set extra strong passwords for those accounts that are crucial to you (email accounts, social media accounts, online banking accounts, etc.) and make it memorable, so you can use it anytime you’d like.

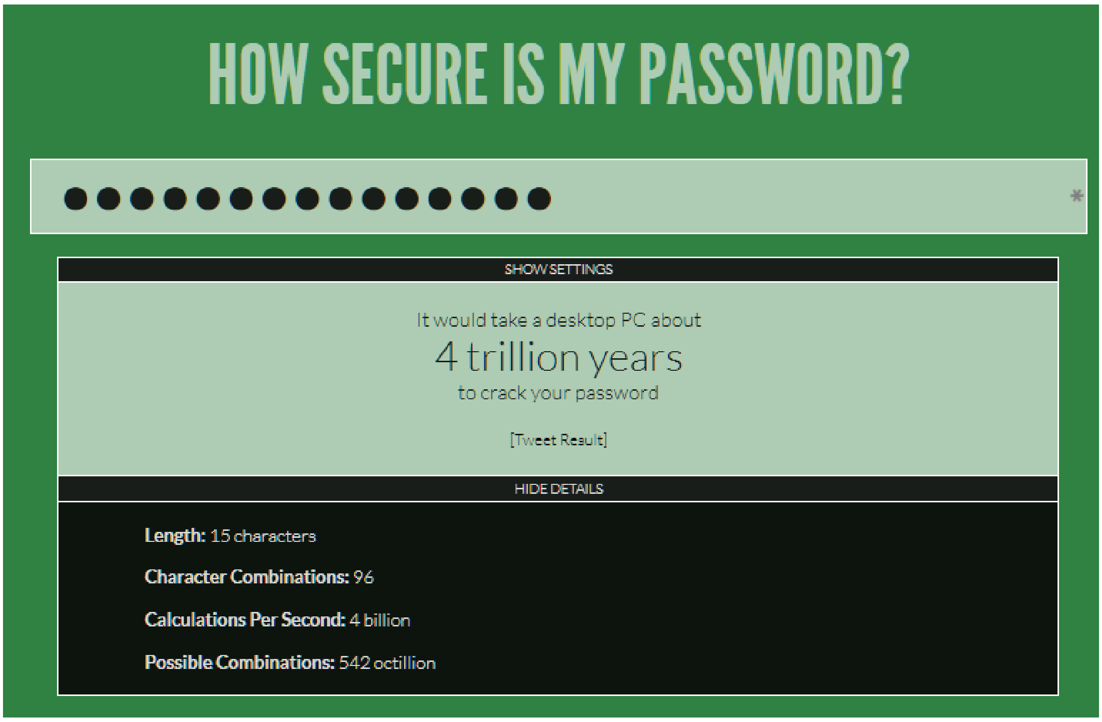
Don’t forget to apply step 2 when doing it. It’ll be good exercise for your memory as well.

Step 4. Test your passwords’ strength using howsecureismypassword.net.

This could give you an idea of how dreadfully unsafe your old passwords were and give you a bit of comfort to know that you’re doing the right thing by taking the time to update your credentials.

Here is the result from having tested the password shown as an example above:

Lesson 4



HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●●●●●

SHOW SETTINGS

It would take a desktop PC about
4 trillion years
to crack your password

[Tweet Result]

HIDE DETAILS

Length: 15 characters

Character Combinations: 96

Calculations Per Second: 4 billion

Possible Combinations: 542 octillion

So, you have your new, long and complex passwords. But you have over 150, maybe even 200 accounts.

What now?
Well, now comes the part where you get learn...

How to safely store your passwords in 8 steps

Step 1. Use a password manager.

The reason behind this recommendation is: you'll only have to remember one strong password and all your other passwords will be protected from keylogging and other credential-sniffing tool that cyber criminals might use.

Best free password management applications:
https://lastpass.com/
https://www.passwordbox.com/
https://identitysafe.norton.com/
https://www.wwpass.com/products/blackbook-password-manager/

Best paid password management applications:
https://www.dashlane.com/passwordmanager
https://lastpass.com/features_premium.php
https://www.stickypassword.com/free-vs-premium
http://www.roboform.com/why-everywhere
https://www.intuitivepassword.com/
https://keepersecurity.com/download.html
http://www.roboform.com/download

Step 2. **If you want to go the extra mile, you can even consider using more than one password manager application,** thus lowering the potential damage if one password-storing service gets compromised (that's a possibility too). Don't put all your eggs in one basket, as they say.

You might argue that these apps and services are prone to vulnerabilities as well, and that's very true, but it's much better than using the same password for every service you use. Plus, password security is their business, so rest assured that they know a thing or two about information security.

Step 3. Where it's available, **two-factor authentication** is another great safeguard against cyber attacks.

Using this option is especially important when it comes to the critical accounts we talked about earlier.

How to turn on 2-step verification on Google:
https://support.google.com/accounts/answer/180744?hl=en&ctx=ch_b%2F0%2FSmsAuthLanding

How to turn on Login Approvals on Facebook:
https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920

How to turn on two-step verification on Yahoo:
https://help.yahoo.com/kb/turn-two-step-verification-sln5013.html

How to set up Logic Verification on Twitter:
https://blog.twitter.com/2013/getting-started-with-login-verification

How to turn on two-step verification on Dropbox: https://www.dropbox.com/en/help/363

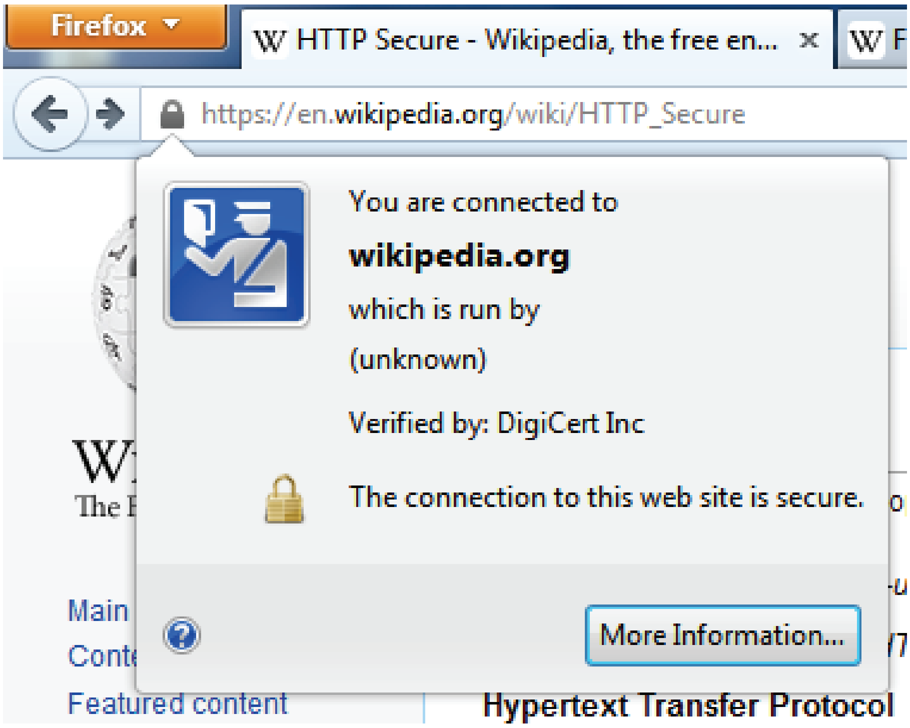
You can also use this list to verify is other services you use offer 2-step verification: **https://twofactorauth.org/**.

Step 4. **Be especially careful with the passwords you use for logging into financial services,** such as your online banking account.

Try not to type these passwords, and try to use a multi-layered protection system against cyber criminals who are after your money (even if you don't have millions in the bank, trust me, they're still after it).

Step 5. Make sure that, when you log into an especially important account, the website has **added protection through HTTPS.**

HTTPS is communications protocol for secure communication over a computer network. Its value comes from the fact that it provides bidirectional encryption of communications between a user and server, which protects you against cyber criminal attacks such as eavesdropping.



You are connected to

wikipedia.org

which is run by

(unknown)

Verified by: DigiCert Inc

The connection to this web site is secure.

Firefox
HTTP Secure - Wikipedia, the free en...
https://en.wikipedia.org/wiki/HTTP_Secure
More Information...
Main
Conte
Featured content
Hypertext Transfer Protocol

If a website you're visiting does not have HTTPS enabled, you'd better double check its safety and see if you're sure you want to enter your credentials there. Additionally, you might not want to store your credit card details in that account either.

Step 6. Keep your browser and vulnerable software updated.

Every time you don't have time to perform an update for one of your browsers or on a software such as Java, Adobe Reader or Adobe Flash, a cyber criminal is taking advantage of a flaw left uncorrected (ad potentially unleashing a Zero Day virus on you).

Updates are not only used to deliver better functionality, but security patches as well!

Step 7. Change your passwords frequently.

Even if you've set strong passwords, keeping things fresh always helps.

By putting together this routine and applying it constantly, you'll discover a new way of keeping safe online, which will give you peace of mind and a sense of comfort.

Step 8. Don't compromise yourself.

Sometimes, human error is the biggest liability in our data's security, so try to keep paying attention to how you share passwords.

When you're either delegating work, go for a vacation or a sick leave, give access to business partners, or even when a colleague asks you for a passwords, chose the safe way to do it.

You can share passwords safely through a password management service and some apps even define levels of access (which are pretty common nowadays), so take full advantage of those options.

And also **be aware of the people around you**. Someone might just look over your shoulder and check out your password. Be mindful of your surroundings, both when you’re online and offline.

Can’t anyone figure out something better than passwords?

They haven’t yet. So passwords will be around for a while, that’s for sure. Until we’ll start using **biometric technology** or a groundbreaking innovation comes into play, we will still rely on this method of authentication. **So we’d better do it right!**

To end things on a funny, but educative note, here’s Edward Snowden talking about password security with John Oliver. It’s a 3 minute video that could, perhaps, talk you into making some changes, if I haven’t managed to persuade you until this point.

Lesson 4

https://www.youtube.com/watch?v=yzGzB-yYKcc

Stay safe!

PS: There are even some free tools you can use to check and see if your passwords for different accounts have been compromised or not:
https://breachalarm.com/
https://pwnedlist.com/query
https://haveibeenpwned.com/

Use them wisely!

Lesson 5 /19

How do I choose the best antivirus: We have just the thing for you

Lesson 5

In the previous lesson, we provided some useful insights and solutions on how you can create a password and how important it is to have a strong one for your online accounts.

Now, it's time for us to approach **one of the most important lessons of our course** and finally answer a vital question:

How can you choose the best antivirus software?

I know there are many antivirus solutions on the market and you probably have difficulties in picking the right product for your system.

And I really understand this. Though I've been working for some time in the IT industry, when I see so many security products, even I am a bit puzzled on what I should select.

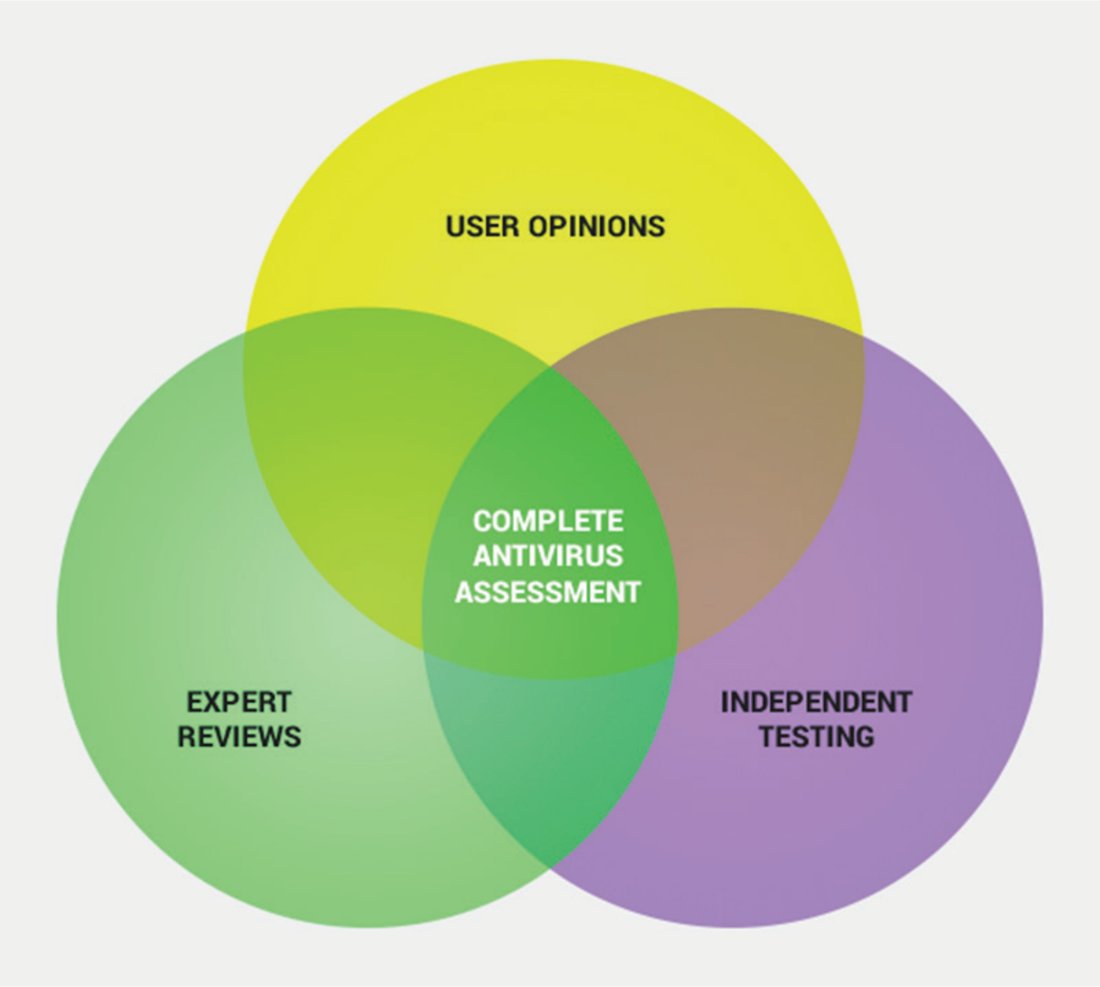
So what is the best antivirus for my computer?

Since we're dealing with so much confusing information, I believe it's a good idea to organize the main sources of data, before I explain each area of interest and how it is useful for your antivirus research.

Here are 3 sources where you can find the information you need:

- **User opinions**
- **Expert reviews**
- **Independent testing**

Lesson 5



User opinions

First of all, **you are not the first who asked this question.** And for sure, you won't be the last. For this reason, one of the easiest ways to find the best antivirus program is **to**

check what other users have to say in security forums reviews and topics from various websites.

Important!
Before I proceed, I must underline that a user's opinion should be taken into account only after analyzing the posting history and only after checking there's no obvious bias for a security product.

Security forums

Some of the best places to find user opinions and product reviews on security solutions and antivirus software on the market are **the good old security forums in the IT industry.**

For example, the links below will send you to some of the best security forums in the online, where you can find a great number of user reviews and good (or bad) experiences users encountered with security products:

The Community Video Reviews – a forum which contains video reviews and tests antivirus products
Windows Secrets – Security & Scams
Wilders Security Forums – Security Products
CyberPower Forum – Anti-virus
Bleeping Computer – Anti-Virus and Anti-Malware Software

Quora

This website is based on **questions and answers** that become useful to the community of users. You can ask a question and receive answers or you can find answers to questions that have already been asked.

The website is designed so that you may be able to find quickly your areas of interest. To go fast to the security areas, insert in the Search bar the following: **Computer Security, Anti-Virus Software** or **Internet Security** will take you to the designated topics:

- Computer Security
- Anti-Virus Software
- Internet Security

As you can see, **these topics are followed by thousands of people**, so it should not be too difficult to find what you're looking for.

Yahoo Answers

This website is another place where you can share your knowledge on a variety of topics. It is at the same time a good place to find questions and answers for Internet and computer related security subjects.

That’s why I recommend posing your security questions here, like “***What’s the Best Antivirus?***”

For specific areas on Internet security, check these categories:

- Software
- Internet
- Security

Trustpilot

You read the available user reviews and the experiences others encountered after purchasing a certain antivirus. In this process, you probably changed your mind a few times.

But now that you have decided on the best product, maybe it’s time to see what others have to say about the site they used to purchase the product.

For this, you can simply access the Trustpilot site and insert the website you want to use for your purchase in the required field. The search results will indicate the **good or bad experiences** people had with that website and it will give you a better perspective on this whole process.

Lesson 5

Expert Reviews

PC Magazine

PC Magazine is not just a testing agency, it is a complete guide to computers, a place where you find computer and Internet related products and services.

To check what security solution you should choose, access their website and use one of the following options:

Take a look at the top right corner and insert in the search field **Best Antivirus**. (It should already be placed there for you).

This is the easiest way to reach Neil Rubenking's article, **Top Antivirus 2016**, where you can find 5 antivirus products selected as the best for 2015.

Here are some criteria you can use to choose the right AV product for you:

In the **Reviews** section, you have a few options to select the **price** you want to pay, the **company** you prefer or the **category** you need. The Category is useful if you look for something different, like a Parental Control product or an antispam tool.

Here again, the easiest way is to go to **Best Antivirus Software** tab in order to access the same article by Neil Rubenking, **The Best Antivirus Utilities for 2016**.
If you take a quick look at the article, you notice the 5 security products are **Webroot SecureAnywhere AntiVirus** (2015), **Bitdefender Antivirus Plus 2016, McAfee AntiVirus Plus 2016, Kaspersky Anti-Virus** (2016) **and Trend Micro Antivirus+ Security 2016**. For each of them, you can see there is a review available.

If you access the review for the products, you will notice the available price, and a few final conclusions (Pros, Cons and Bottom Line) in case you don't have time to read the article.

If you continue to scroll down, you can check the main security features that were put to the test:

- malware blocking
- malicious URL blocking
- phishing detection
- privacy protection
- additional features

So, let's summarize this:

1. You have found the 5 best antivirus products.

2. You read the reviews. I know, it takes time, but it is an important decision.
3. You compare the products. Maybe your first selection criterion is the price. Or it is malware blocking capabilities.
4. You order to product and keep your system safe.

If you are in doubt about a certain product, you can see that most security products nowadays come with a **trial testing mode**, where you can use it for a month or so, and then make up your mind.

We recommend using the **trial period** for any product, because some of them may protect you very well, but they may affect your system's performance. And this is something you learn after a few weeks.

It's no problem if you test more than one security product, simply **remember to keep only one of them on the system in any given period**. Having more than one security product on the system leads to conflicts, slowdowns or even system crashes, since they use the same system resources.

Before you install another product, make sure you have removed completely the previous software using the uninstall tool provided by the company. **Choose wisely**.

Gizmo's Freeware – Best Free Antivirus Software

This website is highly recommended for its security evaluation of free antivirus products. Though I recommend using a paid antivirus product, I need to mention there are out there very good free products that might just cover your security needs. Therefore, use the link above and check the presented solutions for a time, before you decide to go with a paid antivirus product.

Tom's Guide – Best Antivirus Software and Apps 2015

Another important security website to check if you are interested in online protection. The link above will send you to another antivirus evaluation, where only the best products have been taken into account. At the same time, you can also take a look at the free antivirus products tested.

Softpedia – Antivirus

Softpedia comes with a high number of security solutions, from very well established solutions to others, which are less known by the large public. Nevertheless, I think you should give them a chance and take a look at them. Maybe this is where you'll find your security solution.

PC Advisor – Test Centre

The test centre from PC Advisor puts to the test about 21 antivirus products in the market for the UK public. That doesn't mean you can't check them out for yourself and decide if one of them is good for you too.

Independent testing

We have reached the major certification and testing agencies, and it is important to see what they have to say about what is the best antivirus you can choose. After all, they are in business for some years and they can't afford to lose credibility, so checking these places should give you a pretty good idea on what to select.

Important!
We need to make sure the antivirus tests are as objective as possible and respect some fundamental principles of testing. For this reason, I invite you to take a look at this important paper from **Anti-Malware Testing Standards Organization:** AMTSO Fundamental Principles of Testing.

To simplify things, we will demonstrate briefly how you can find the best antivirus for your Windows operating system.

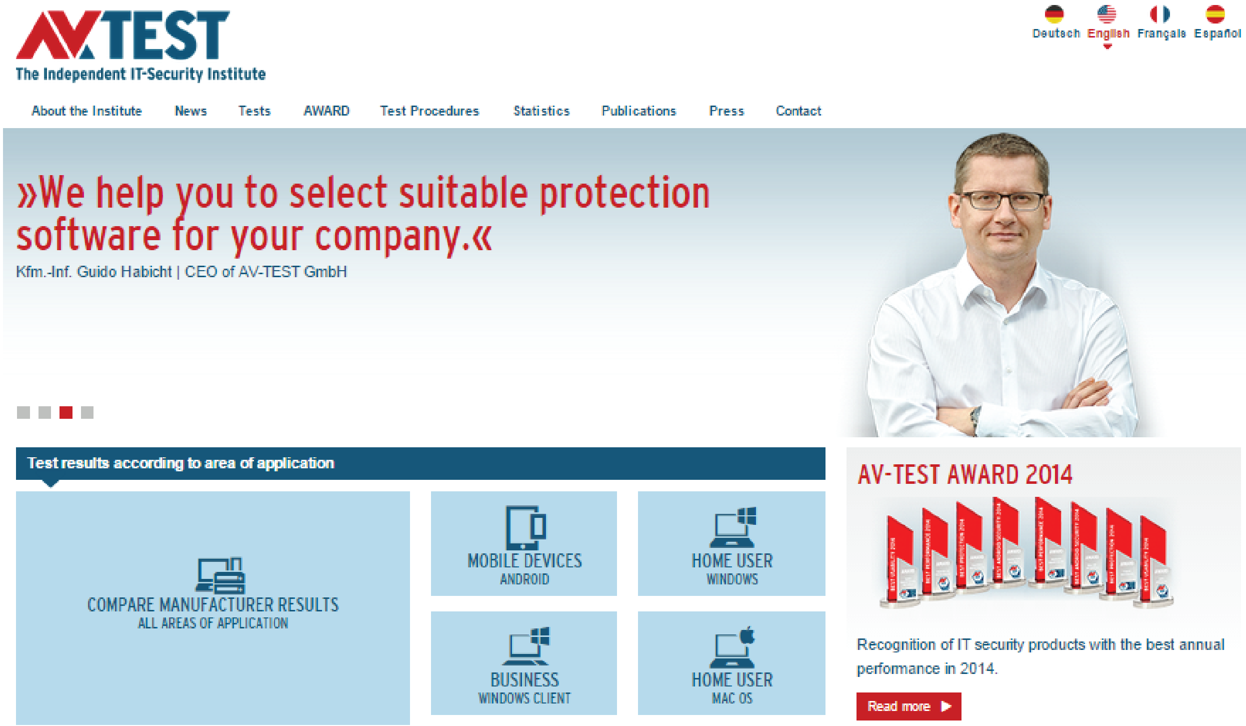
Lesson 5

AV-Test

This testing agency is an independent service provider in IT security that analyzes the latest malware, using the best security solutions available and informs the public on the top-quality results.

To check what security solution you should choose, access their website and follow these steps:

1. Right in front of you, there should be **Test results according to area of application.**



»We help you to select suitable protection software for your company.«

Kfm.-Inf. Guido Habicht | CEO of AV-TEST GmbH

Test results according to area of application

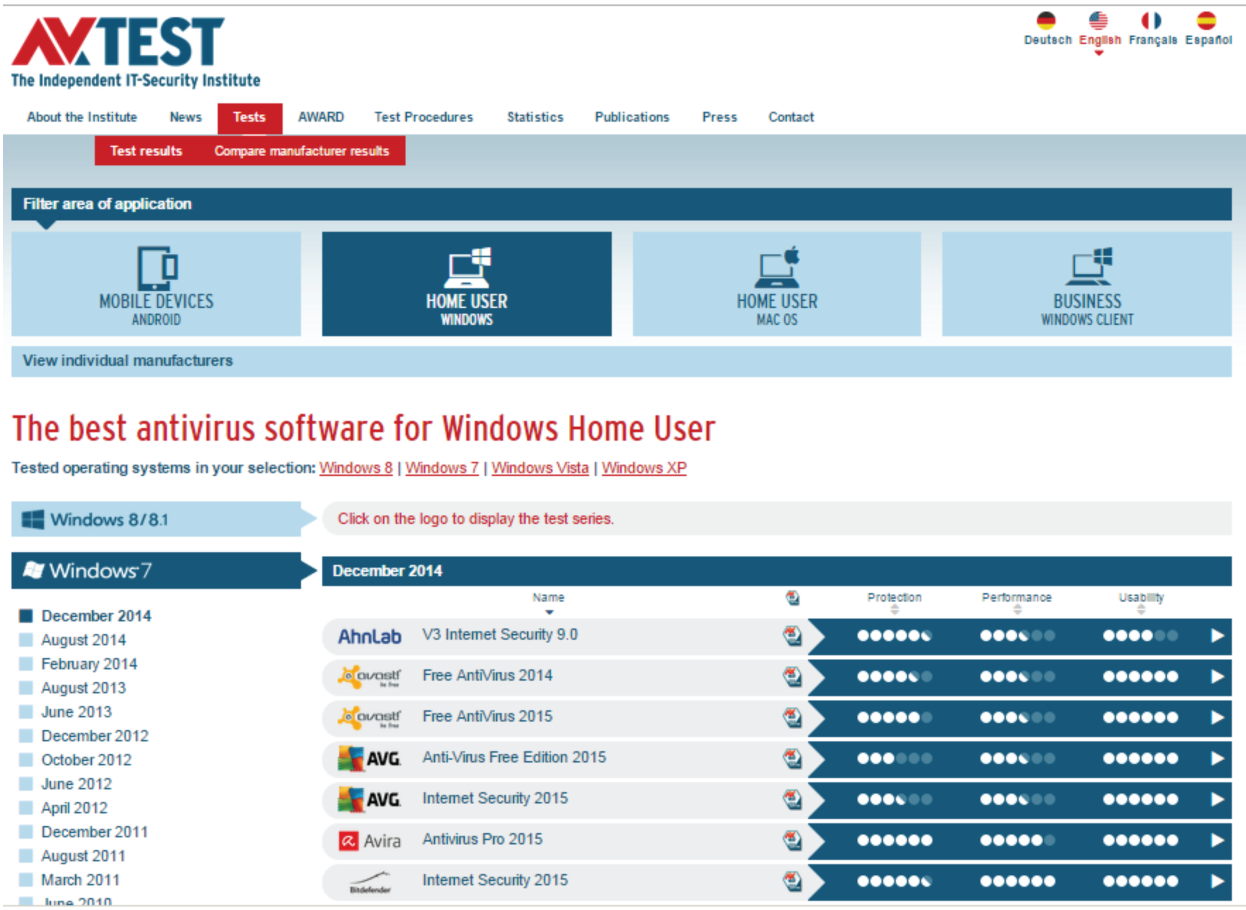
AV-TEST AWARD 2014

Recognition of IT security products with the best annual performance in 2014.

Access **Home User Windows.**

Lesson 5

2. In the new window, select your Windows operating system and from the left column, choose the latest test results period. Then take a look at the security products displayed.



The best antivirus software for Windows Home User

Tested operating systems in your selection: Windows 8 | Windows 7 | Windows Vista | Windows XP

Click on the logo to display the test series.

December 2014

	Name	Protection	Performance	Usability
AhnLab	V3 Internet Security 9.0	●●●●●◐	●●●◐○○	●●●●○○
avast!	Free AntiVirus 2014	●●●●◐○	●●●◐○○	●●●●●●
avast!	Free AntiVirus 2015	●●●●●○	●●●◐○○	●●●●●●
AVG	Anti-Virus Free Edition 2015	●●●○○○	●●●◐○○	●●●●●●
AVG	Internet Security 2015	●●●◐○○	●●●◐○○	●●●●●●
Avira	Antivirus Pro 2015	●●●●●●	●●●●●○	●●●●●●
Bitdefender	Internet Security 2015	●●●●●◐	●●●●●●	●●●●●●

As you can see in the list, there are a great number of products.

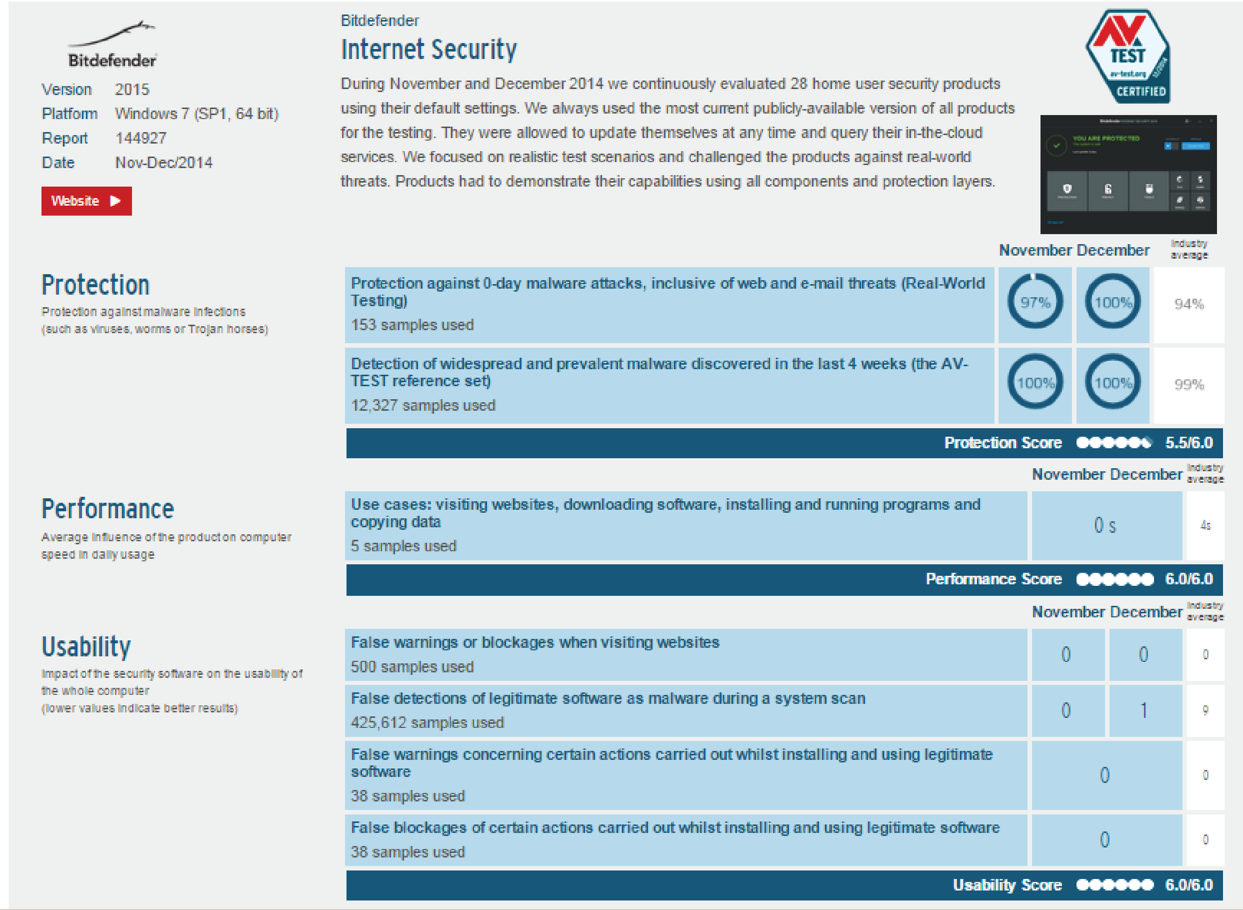
If we take a look at the top of the list, you notice there are 3 main criteria:

Lesson 5

- **Protection**
- **Performance**
- **Usability**

For each criterion, there are 6 maximum points a product can obtain.

3. Let’s choose for our example, ***Bitdefender Internet Security 2015.***



Bitdefender

Version	2015
Platform	Windows 7 (SP1, 64 bit)
Report	144927
Date	Nov-Dec/2014

Website ▶

Bitdefender

Internet Security

During November and December 2014 we continuously evaluated 28 home user security products using their default settings. We always used the most current publicly-available version of all products for the testing. They were allowed to update themselves at any time and query their in-the-cloud services. We focused on realistic test scenarios and challenged the products against real-world threats. Products had to demonstrate their capabilities using all components and protection layers.

AV TEST av-test.org CERTIFIED

Protection

Protection against malware infections (such as viruses, worms or Trojan horses)

	November	December	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 153 samples used	97%	100%	94%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 12,327 samples used	100%	100%	99%
Protection Score ●●●●●◐ 5.5/6.0			

Performance

Average influence of the product on computer speed in daily usage

	November December	Industry average
Use cases: visiting websites, downloading software, installing and running programs and copying data 5 samples used	0 s	4s
Performance Score ●●●●●● 6.0/6.0		

Usability

Impact of the security software on the usability of the whole computer
(lower values indicate better results)

	November	December	Industry average
False warnings or blockages when visiting websites 500 samples used	0	0	0
False detections of legitimate software as malware during a system scan 425,612 samples used	0	1	9
False warnings concerning certain actions carried out whilst installing and using legitimate software 38 samples used	0		0
False blockages of certain actions carried out whilst installing and using legitimate software 38 samples used	0		0
Usability Score ●●●●●● 6.0/6.0			

4. In the list, the following criteria appear:

Protection – Protection against malware infections, which include 0-day malware attacks, including web and email threats

Performance – Average influence of the product on computer speed in daily usage

Usability – Impact of the security software on the usability of the whole computer

To have an idea on each data, you can take a look at the right where the **Industry average** appears.

If you are not sure about a certain product, you can select from the top menu **Tests> Compare manufacturer results.**

This way, you can compare the rest results of several antivirus products and choose the best for your operating system.

AV Comparatives

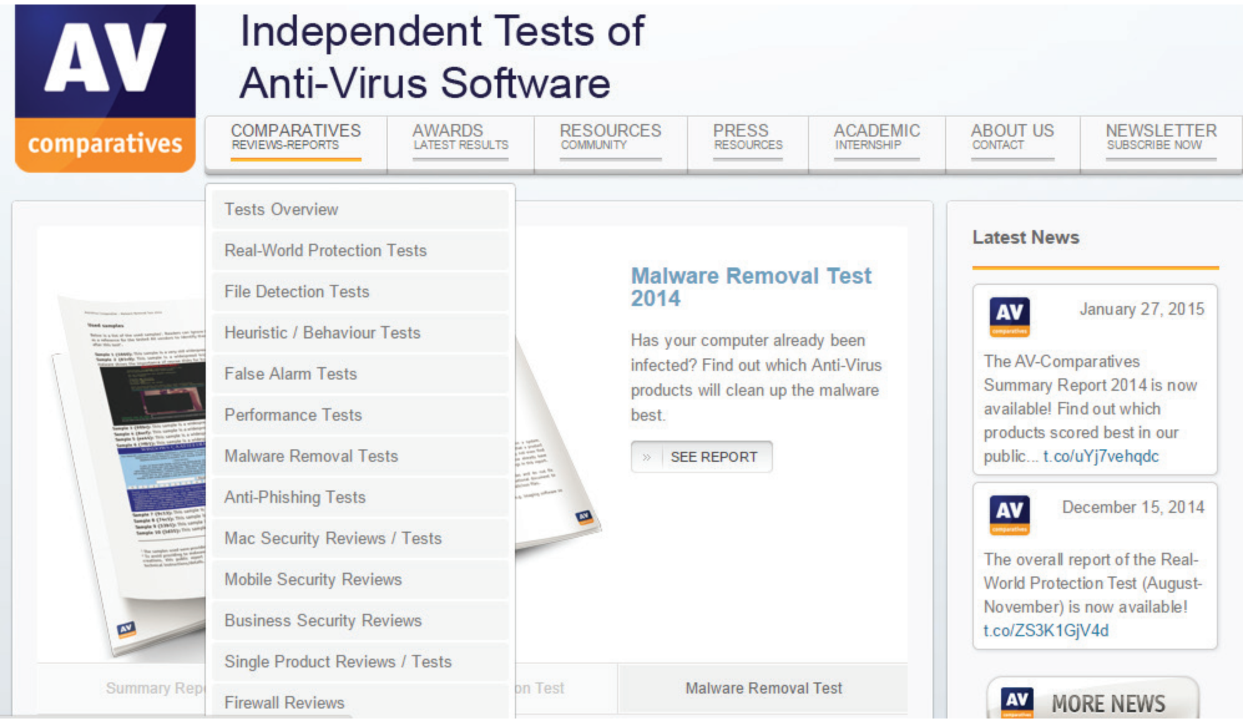
AV Comparatives is an Austrian based testing agency that assesses popular antivirus solutions and releases

Lesson 5

accurate reports and charts. To check what security solution you should choose, access their website and use one of the following options:

You can notice in the top menu a few tests that were run on the antivirus products:

- Real-World Protection Tests
- File Detection Tests
- Heuristic/Behaviour Tests
- False Alarm Tests
- Performance Tests
- Malware Removal Tests
- Anti-Phishing Tests



Malware Removal Test 2014

Has your computer already been infected? Find out which Anti-Virus products will clean up the malware best.

January 27, 2015

The AV-Comparatives Summary Report 2014 is now available! Find out which products scored best in our public... t.co/uYj7vehqdc

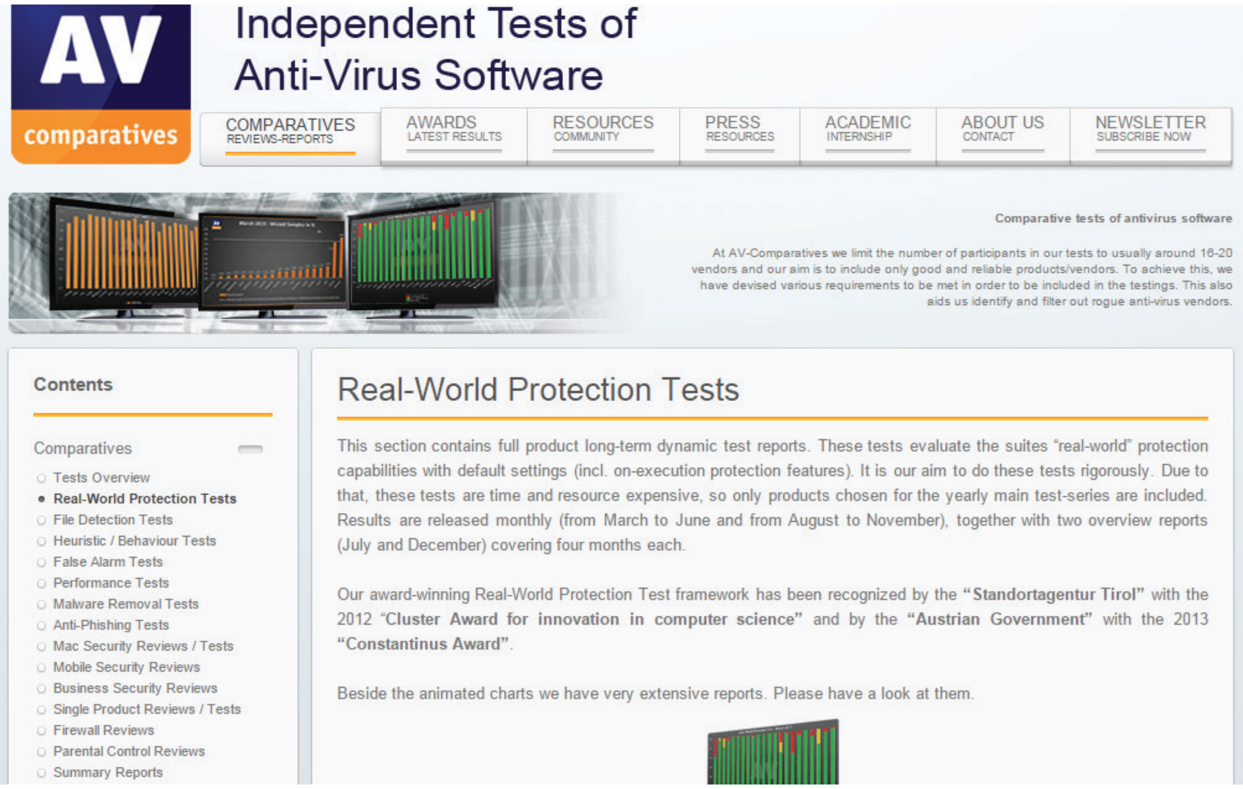
December 15, 2014

The overall report of the Real-World Protection Test (August-November) is now available! t.co/ZS3K1GjV4d

Lesson 5

Though I recommend taking a look at all the available tests, I think that starting with the **Whole Product Dynamic “Real-World” Protection** and **Performance** tests, is a good place to start. These 2 tests will give you most certainly a good idea on what the best security product is for your system.

Real-World Protection Test



Comparative tests of antivirus software

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and our aim is to include only good and reliable products/vendors. To achieve this, we have devised various requirements to be met in order to be included in the testings. This also aids us identify and filter out rogue anti-virus vendors.

Contents

Comparatives

- Tests Overview
- **Real-World Protection Tests**
- File Detection Tests
- Heuristic / Behaviour Tests
- False Alarm Tests
- Performance Tests
- Malware Removal Tests
- Anti-Phishing Tests
- Mac Security Reviews / Tests
- Mobile Security Reviews
- Business Security Reviews
- Single Product Reviews / Tests
- Firewall Reviews
- Parental Control Reviews
- Summary Reports

Real-World Protection Tests

This section contains full product long-term dynamic test reports. These tests evaluate the suites “real-world” protection capabilities with default settings (incl. on-execution protection features). It is our aim to do these tests rigorously. Due to that, these tests are time and resource expensive, so only products chosen for the yearly main test-series are included. Results are released monthly (from March to June and from August to November), together with two overview reports (July and December) covering four months each.

Our award-winning Real-World Protection Test framework has been recognized by the **“Standortagentur Tirol”** with the 2012 “**Cluster Award for innovation in computer science”** and by the **“Austrian Government”** with the 2013 **“Constantinus Award”**.

Beside the animated charts we have very extensive reports. Please have a look at them.

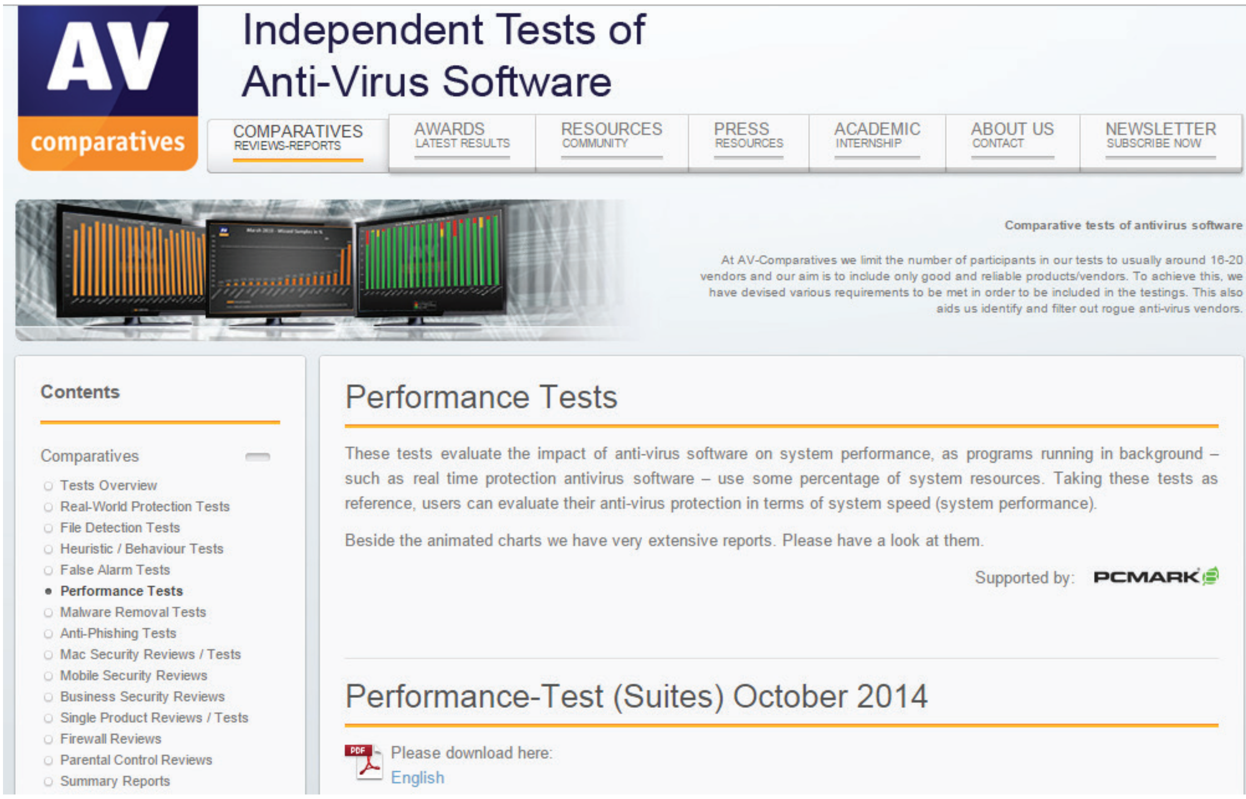
This is probably the most important test you need to take into consideration, because it indicates the Protection Rate achieved by a certain product.

Lesson 5

To quote the guys who run this test: “all protection features of the product can be used to prevent infection – not just signatures or heuristic file scanning.”

Therefore, consider the test and then take a look at page 9 to check the results and compare the products that were put to the test. Look at those products that got over 99% in protection rate score.

Performance Test



Independent Tests of Anti-Virus Software

Comparative tests of antivirus software

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and our aim is to include only good and reliable products/vendors. To achieve this, we have devised various requirements to be met in order to be included in the testings. This also aids us identify and filter out rogue anti-virus vendors.

- Tests Overview
- Real-World Protection Tests
- File Detection Tests
- Heuristic / Behaviour Tests
- False Alarm Tests
- **Performance Tests**
- Malware Removal Tests
- Anti-Phishing Tests
- Mac Security Reviews / Tests
- Mobile Security Reviews
- Business Security Reviews
- Single Product Reviews / Tests
- Firewall Reviews
- Parental Control Reviews
- Summary Reports

Performance Tests

These tests evaluate the impact of anti-virus software on system performance, as programs running in background – such as real time protection antivirus software – use some percentage of system resources. Taking these tests as reference, users can evaluate their anti-virus protection in terms of system speed (system performance).

Beside the animated charts we have very extensive reports. Please have a look at them.

Supported by:

Performance-Test (Suites) October 2014

Please download here:
English

This test gives an indication on the system performance while using a certain Internet security product. Nevertheless, users are encouraged to test a product on their own system.

To give you a clue on the system performance, the test run the following activities:

- file copying
- archiving/ unarchiving
- encoding
- installing/ uninstalling apps
- launching apps
- downloading

And the most important element was that **PC Mark 8 Professional Testing Suite** was also used to provide an industry recognized performance test.

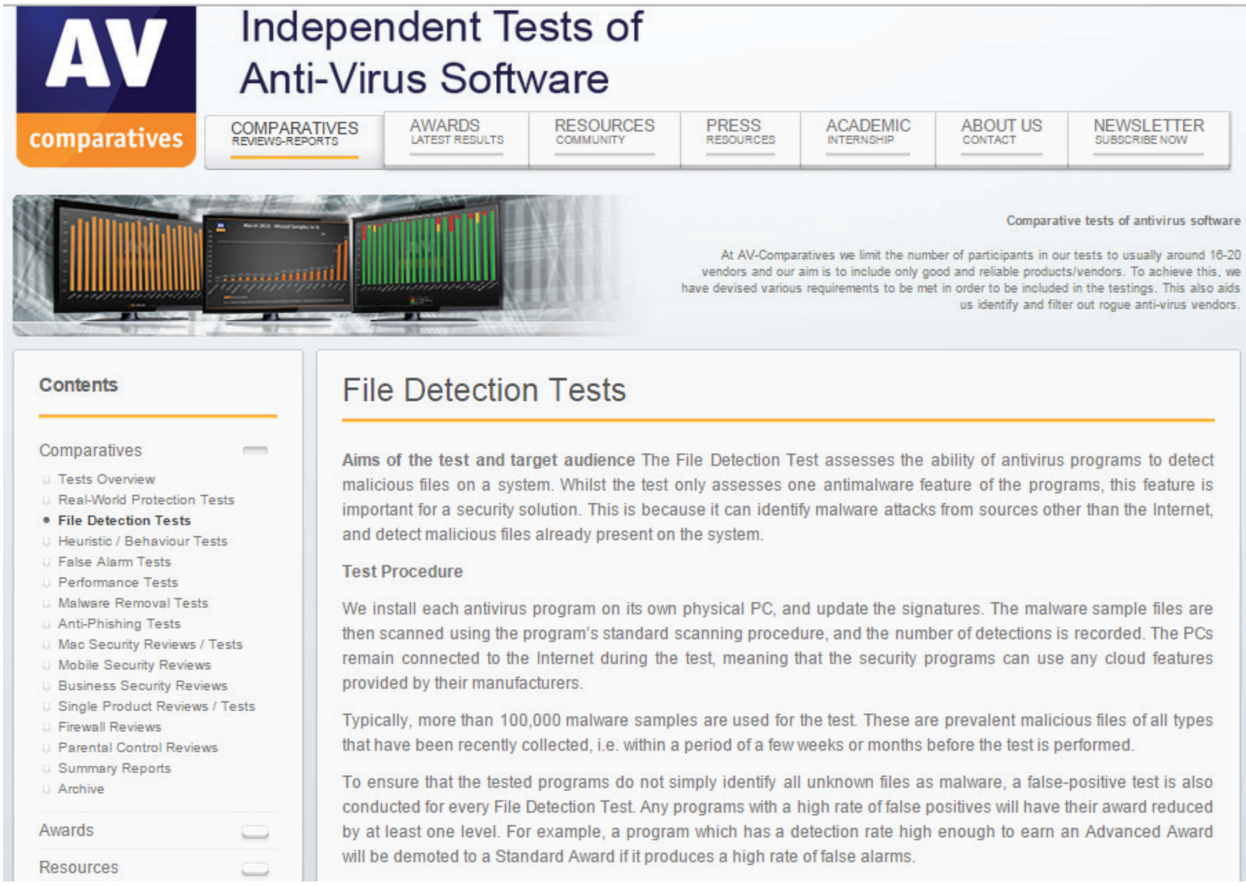
Though I recommend going through the entire test, a simple look at pages 9 and 10 will give you an idea on what security products are in the “green” zone.

For example, the overview of performance scores from page 9 will shed some light on each product performance in file copying, archiving, installing, encoding, launching apps and downloading operations. Scroll down to page 10 and you can see the PC Mark 8 points achieved by each software.

Lesson 5

If you are still not convinced on a product's abilities to keep you safe from malware, I recommend running another 2 additional tests: File Detection Test and Heuristic/ Behaviour test.

File Detection Test



Independent Tests of Anti-Virus Software

Comparative tests of antivirus software

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and our aim is to include only good and reliable products/vendors. To achieve this, we have devised various requirements to be met in order to be included in the testings. This also aids us identify and filter out rogue anti-virus vendors.

Contents

Comparatives

- Tests Overview
- Real-World Protection Tests
- **File Detection Tests**
- Heuristic / Behaviour Tests
- False Alarm Tests
- Performance Tests
- Malware Removal Tests
- Anti-Phishing Tests
- Mac Security Reviews / Tests
- Mobile Security Reviews
- Business Security Reviews
- Single Product Reviews / Tests
- Firewall Reviews
- Parental Control Reviews
- Summary Reports
- Archive

Awards

Resources

File Detection Tests

Aims of the test and target audience The File Detection Test assesses the ability of antivirus programs to detect malicious files on a system. Whilst the test only assesses one antimalware feature of the programs, this feature is important for a security solution. This is because it can identify malware attacks from sources other than the Internet, and detect malicious files already present on the system.

Test Procedure

We install each antivirus program on its own physical PC, and update the signatures. The malware sample files are then scanned using the program's standard scanning procedure, and the number of detections is recorded. The PCs remain connected to the Internet during the test, meaning that the security programs can use any cloud features provided by their manufacturers.

Typically, more than 100,000 malware samples are used for the test. These are prevalent malicious files of all types that have been recently collected, i.e. within a period of a few weeks or months before the test is performed.

To ensure that the tested programs do not simply identify all unknown files as malware, a false-positive test is also conducted for every File Detection Test. Any programs with a high rate of false positives will have their award reduced by at least one level. For example, a program which has a detection rate high enough to earn an Advanced Award will be demoted to a Standard Award if it produces a high rate of false alarms.

It is an important element you need to consider before purchasing an antivirus product.

As in the other tests, the default settings were used and the on-access scanning is taken into consideration. At the same time, an additional False Positives test has been run, which is something you should consider in your final conclusion.

Again, though I recommend reading the entire test, if you take a quick look at page 7, you will notice the detection rates' results. Here you can take into consideration the software that obtained at least a 99% score. Just to be on the safe side, scroll down to page 8 and see how the number of FPs and of course that the fewer they are, the better.

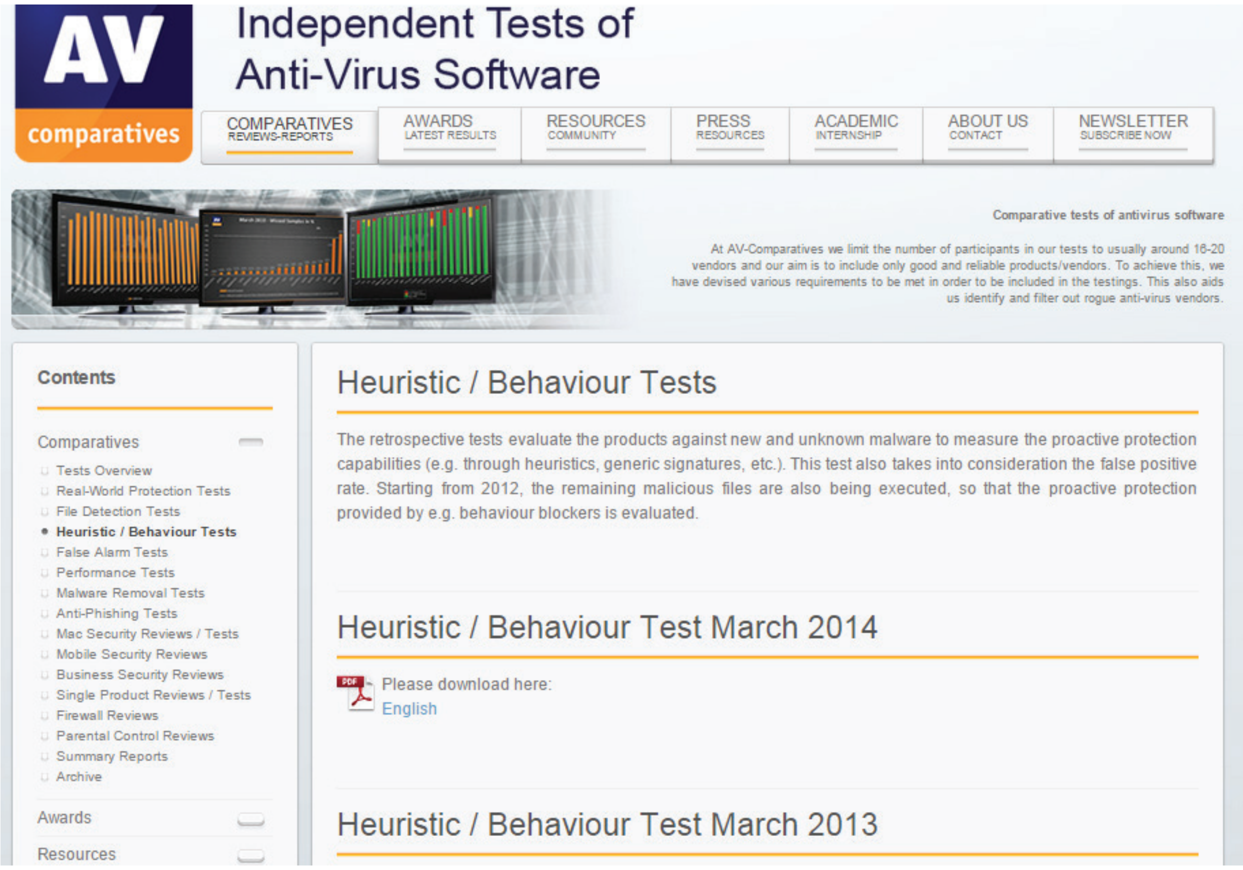
Heuristic/Behaviour (or Retrospective/Proactive)

This test is run by AV Comparatives once a year and includes behavioral routines, which evaluate the **proactive protection capabilities** of the products.

The main idea behind this test is to **evaluate how antivirus products are able to detect new malware threats** using heuristic techniques or behavioral protection measures.

Since new malware appears every day and there is always a time frame in which you are not protected, that is until the malware signature is sent to your antivirus

Lesson 5



Independent Tests of Anti-Virus Software

Comparative tests of antivirus software

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and our aim is to include only good and reliable products/vendors. To achieve this, we have devised various requirements to be met in order to be included in the testings. This also aids us identify and filter out rogue anti-virus vendors.

Heuristic / Behaviour Tests

The retrospective tests evaluate the products against new and unknown malware to measure the proactive protection capabilities (e.g. through heuristics, generic signatures, etc.). This test also takes into consideration the false positive rate. Starting from 2012, the remaining malicious files are also being executed, so that the proactive protection provided by e.g. behaviour blockers is evaluated.

Heuristic / Behaviour Test March 2014

Please download here:
English

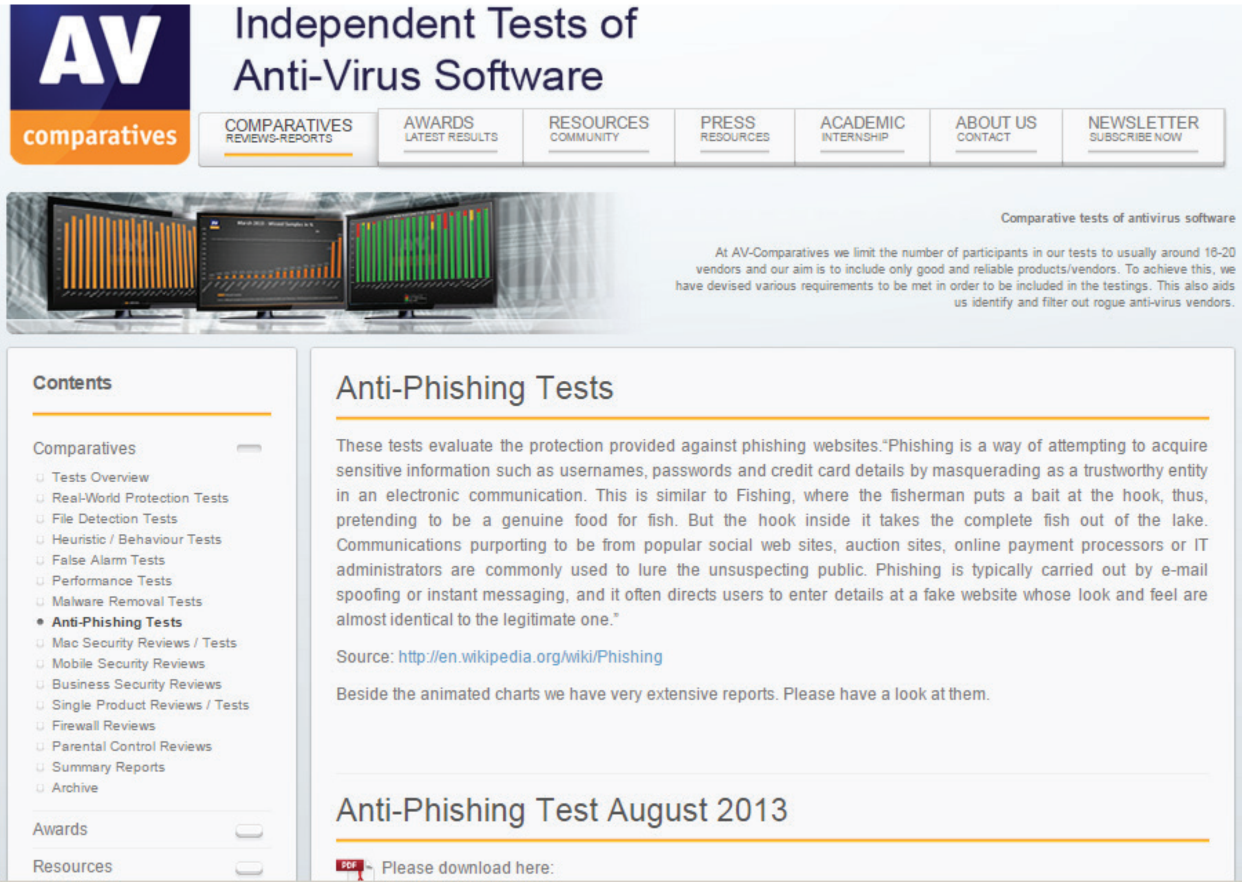
Heuristic / Behaviour Test March 2013

product, **this heuristic technology becomes the last line of defense against malware**, and therefore it is not something you should ignore.

If you don’t have the time to go through the entire test, take a look at page 5 and again look for the products in the “**green**” area, which means these software solutions are capable to keep the system safe from new malware threats.

Lesson 5

Anti-Phishing Test



Independent Tests of Anti-Virus Software

Comparative tests of antivirus software

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and our aim is to include only good and reliable products/vendors. To achieve this, we have devised various requirements to be met in order to be included in the testings. This also aids us identify and filter out rogue anti-virus vendors.

Anti-Phishing Tests

These tests evaluate the protection provided against phishing websites."Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to Fishing, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one."

Source: http://en.wikipedia.org/wiki/Phishing

Beside the animated charts we have very extensive reports. Please have a look at them.

Anti-Phishing Test August 2013

Please download here:

This test evaluates the protection against phishing attempts, which usually occur by email or instant messaging, and lure the target into entering sensitive details on fake websites that look similar to the legitimate ones.

As in the previous tests, you can go directly to page 4 and see an overview of the percentages of blocked phishing websites, for each product tested. It is obvious in this case again that the first 3 places are to be considered.

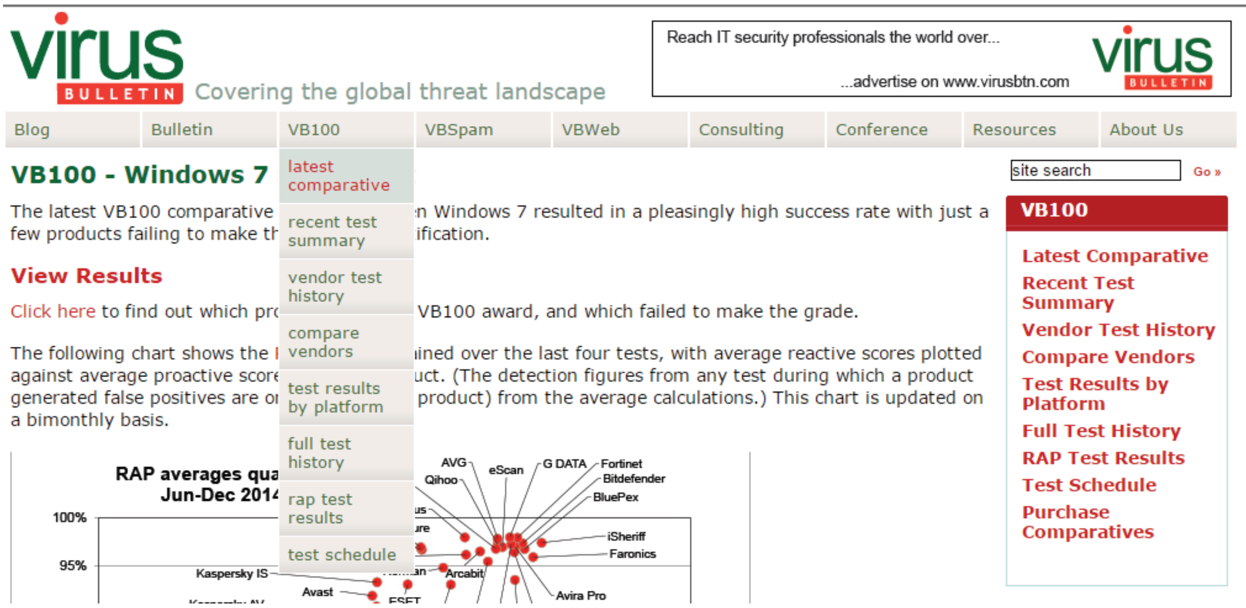
For more information on a security product, you can continue to analyze the other test results in order to make sure you found a good product.

Virus Bulletin

Virus Bulletin is one of the most reliable testing facilities and it frequently features analyses of a great number of anti-virus products, offering an objective point of view for any user that needs the best antivirus product.

Though the website may seem a bit intimidating at first, with that technical feeling all over, you can reach quite easily the comparative tests.

As you enter the website, you need to access **VB100** in the top menu and select “**latest comparative**” from the drop-down menu.



VB100 - Windows 7

The latest VB100 comparative ... n Windows 7 resulted in a pleasingly high success rate with just a few products failing to make th ... ification.

View Results

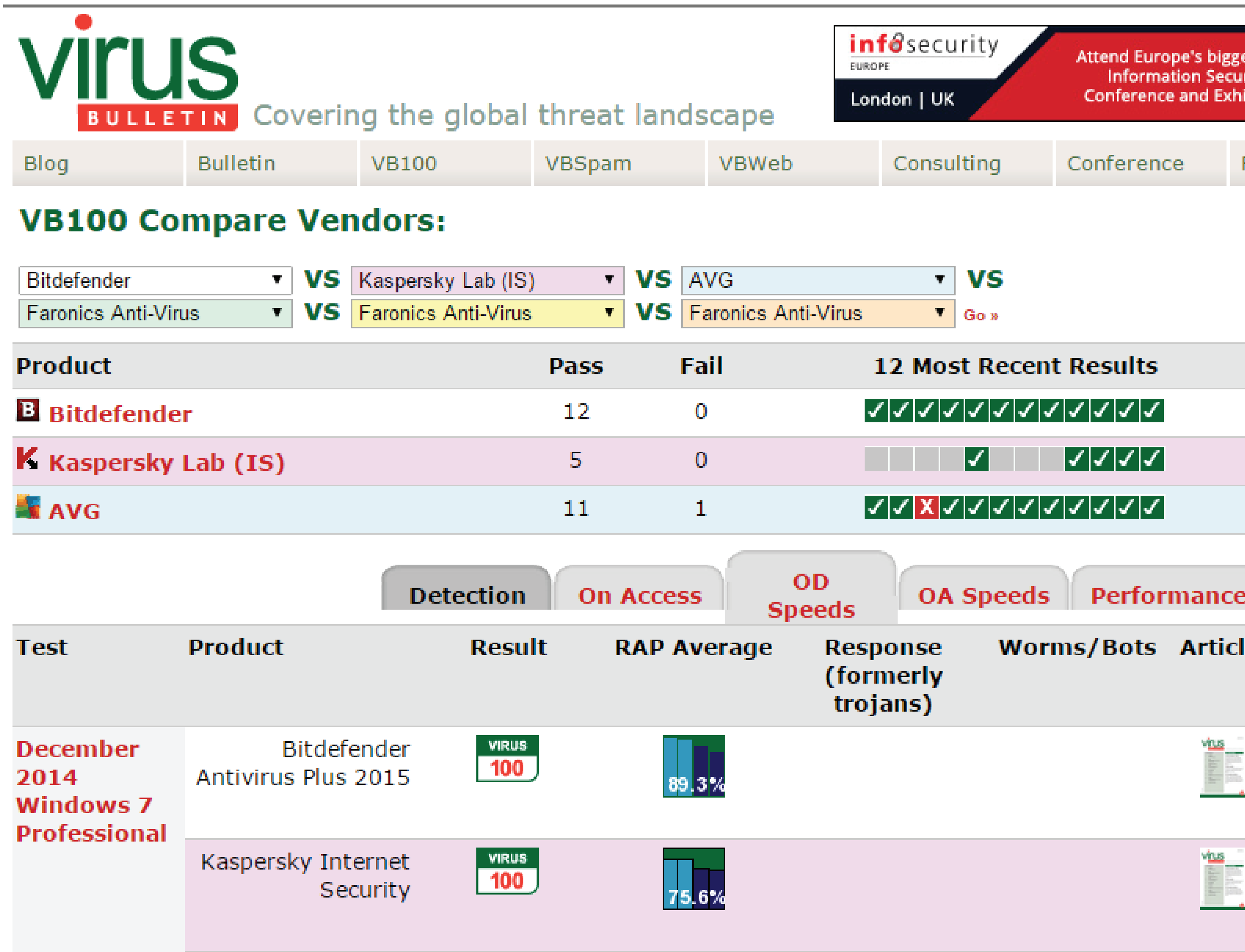
Click here to find out which pr ... VB100 award, and which failed to make the grade.

The following chart shows the ... ined over the last four tests, with average reactive scores plotted against average proactive score ... uct. (The detection figures from any test during which a product generated false positives are o ... product) from the average calculations.) This chart is updated on a bimonthly basis.

Lesson 5

If you scroll down and click “**full Windows 7 report**“, you can read the entire document, which contains many security details, like **detection** score, **False Positives**, **stability** rating, **performance** measures and the **RAP** (Reactive and Proactive) tests.

To make things easier for you, you can go in the same drop down menu and choose “**recent test summary**” or “**compare vendors**” to have a better picture on how each product scored in the test.



virus BULLETIN Covering the global threat landscape

infosecurity EUROPE London | UK Attend Europe's bigge Information Secu Conference and Exhi

Blog | Bulletin | VB100 | VBSpam | VBWeb | Consulting | Conference

VB100 Compare Vendors:

Bitdefender ▾ VS Kaspersky Lab (IS) ▾ VS AVG ▾ VS
Faronics Anti-Virus ▾ VS Faronics Anti-Virus ▾ VS Faronics Anti-Virus ▾ Go »

Product	Pass	Fail	12 Most Recent Results
Bitdefender	12	0	✓✓✓✓✓✓✓✓✓✓✓✓
Kaspersky Lab (IS)	5	0	▢▢▢▢✓▢▢▢✓✓✓✓
AVG	11	1	✓✓✗✓✓✓✓✓✓✓✓✓

Detection | On Access | OD Speeds | OA Speeds | Performance

Test	Product	Result	RAP Average	Response (formerly trojans)	Worms/Bots	Articl
December 2014 Windows 7 Professional	Bitdefender Antivirus Plus 2015	VIRUS 100	89.3%			
	Kaspersky Internet Security	VIRUS 100	75.6%			

This way you can easily compare favorite products by looking at how they behave on Detection, Performance or even Proactive scanning technology.

Dennis Technology Labs

This testing company is one of the most renowned independent evaluation facilities in the IT industry analyzing both consumer and business solutions.

To access the latest security report, access this location and open the latest available test from the Home Anti-Virus Protection, which is at the bottom of the page.

If you don’t want to go through all the report’s data, the first page gives an **Executive Summary**, which offers an idea on the products tested and their scores. Again, the reliable products will appear in the “**green**” area.

In the second page, you can see the conclusion of the report: ***“Which was the best product?“***

You already know this by now:

Your choice of cyber security software can make or break your data protection!

Lesson 5

Antivirus is essential to have, but **it's not enough**, as you'll find out from the next lesson.

So how can you protect your system from advanced threats if AV can't do it?

The answer is simple: by using a cyber threat security suite that is focused on proactive protection. You'll find out more about why next-generation anti-hacking tools are important and why antivirus can no longer cope with current threats in the next lesson.

Lesson 6 /19

Next-gen anti-hacking tools are here to protect you (because antivirus is not enough)

Lesson 6

Our last guide provided useful instructions on how you can choose the best antivirus product for your system.

Now, a new question pops up:

Can a traditional antivirus product protect you from advanced malware attacks launched by cyber-criminal minds?

And since this is an important question, I think you need a straight answer, so here it is:

Though I believe a very good antivirus product can still cover most of your system's security, **the present threats and cyber criminal attacks have the ability to overcome your antivirus's detection system.**

For this reason, you simply need to employ additional weapons in the fight against advanced pieces of malicious code delivered by hackers.

How do cyber criminals evade traditional detection?

I don't want to emphasize the idea that **traditional antivirus is dead**, but only point out to a few simple techniques that are used by anyone who creates a malicious piece of code:

- they **install the** best antivirus **products** and see if they detect the piece of code as being malicious

- they just **upload the piece of code on** Virus Total and see if any antivirus product in the list detects it
- they **use a packer or** obfuscation **capabilities**, which due to their polymorphic abilities evade normal antivirus detection
- antivirus **vendors are slow in updating the malware signatures**

So, how do you stay safe from most online threats, if not all?

10 Steps to Bulletproof Your Digital Security

1. Use a reliable antivirus product

I know, it sounds funny, but **traditional antivirus products are not dead yet**. Or just not yet. You still need a good antivirus to catch most malware, block phishing threats and check web reputation of popular online domains.

Though it is not an easy task to find the best antivirus product from the market, it is still a very useful tool to block most malware threats.

We've covered the how tos of choosing an AV in **lesson 5**, so feel free to go back to it as often as you need to.

2. Stick with your old firewall solution

Though the firewall has been placed lately on that list of ineffective security tools that we can forget about, there are still voices that consider the **time when we still need firewalls is not yet over.**

Though I admit there are limitations to its blocking capabilities, the firewall is still a good tool that you can use to filter your Internet traffic, block communication from an infected machine or online location.

In this case, there is quite a similarity between the antivirus and the firewall. **They both cover some areas of Internet security, but just not all of them.**

3. Use anti-spyware solutions to protect your system

As you already know, spyware is software that monitors your Internet traffic and uses your personal information against you.

In cases where multiple issues appear, like system slow-down, pop-ups when you navigate, new toolbars and random error messages, all these indicate a possible spyware infection.

To stay safe from spyware, you can use a few popular anti-spyware products, like Malwarebytes or Spybot Search and Destroy.

Or, to prevent this type of infection, **follow a few steps**:

- don't click suspicious links in emails from unknown people
- don't click unexpected pop-ups, even from legitimate websites
- don't disclose personal information to strangers on social media platforms
- pay attention to drive-by downloads that could bring spyware on your system

4. Use automatic update tools for your vulnerable applications

Are you using Adobe Flash, Reader or Java on your operating system?

Are you using at least one popular web browser like Google Chrome or Mozilla Firefox?

99% of users will say YES.

"*What does that mean for me?*", you may ask.

By using security holes in unpatched applications, cyber criminals manage to spread exploits that deliver financial and data stealing malware on the affected systems.

For this reason, you always need to have the latest security patches available and this can only be done by using a free solution that does this automatically for you.

5. Use a password manager for your credentials

It is easy to subscribe to a great number of online accounts and forget what passwords you have set. To avoid this issue, most people simply choose using only one or two passwords all the time.

But, this is exactly what hackers count on!

That's because not all these online accounts incorporate high security standards to protect our password. And if they break just one account and find out your password, they can simply use it on all the other online locations.

*Remember **lesson 4***? I hope you've already applied the steps there, so that you can check this off and move on to the next thing!

6. Back-up your system and sensitive information

If you ask security experts their best advice on how to keep sensitive information secure from cyber-criminals, most of them will tell you that a back-up solution is the best option you have.

So, even if your system is blocked by **ransomware** that stops you from accessing it, you can format the system and use your backup to be back on track.

You can use one of the available back-up solutions available or you can keep most important data in the cloud and access it from any location and any device.

Back-up solutions coming your way in **lesson 8**!

7. Maximize your data and financial protection

These security products are designed to detect online threats that normal antivirus products can't remove, like **Zero Day attacks** that a traditional signature based antivirus is not able to block from infecting your system. Most of the time, **these solutions target financial infor-**

mation from the system, like credit card and pin numbers or personal data that we employ on online banking accounts.

In order to get protection against data stealing malware, the solution you need should:

- include a **real-time Internet traffic scanner** that scans all incoming network data for potential malware threats
- provide **malware detection and removal** of malicious code from a system
- contain **online scanning capabilities** that detect malicious software from online pages and legitimate websites

To assure financial security for banking operations and protection against zero day malware, you need an advanced scanning technology that can protect you from the latest threats.

8. Encrypt your important files

By encrypting your personal information you make sure cybercriminals can’t access your confidential data, even if they gain access to your operating system.

You can choose to encrypt files on your local disk or you can choose an online location, which makes things more difficult for any hacker.

Since this is a long topic, I recommend that you **think about encryption as an important part of your online security strategy.**

For example, you can use an encryption program for your files, *but how useful can it be if your password for the program is not that strong?*

Think about encryption as an important part of your online security strategy. And check your inbox for lesson 8 a little down the road for a list of tools you can use.

9. Protect your online traffic by using multiple tools

How do you keep your system safe from online threats?

It is the same question I started this article with, but ***are we closer to the answer?***

To improve your online protection, you cannot rely on a single solution, but you rather need to understand that multiple means and guidelines need to be followed:

- let's start with the **browser**. *Are you using the latest version that contains all the available security patches?*

- *did you know that you can improve your good old browser?*
- *how much are you travelling and need to use* ***public networks and computers?*** In case you do, don't forget to use a private browsing session to go online or at least use a free **proxy server to hide your IP** address from surveillance mechanisms.
- *are you serious about online security and privacy?* Then you need to best tools available out there. To encrypt your online connection, use a VPN solution. Choose the Tor browser to hide your Internet activity by sending your communication through the Tor network of computers.

  Get your browser protection right in **lesson 10**. You're only 4 lessons away!

10. Listen and learn from the best

Though you may rely on one or more security solutions to do the job for you, a set of safety guidelines should be followed. In **lesson 19**, a little further down the road, we'll share some stuff you're probably never thought of (and that you REALLY NEED).

That's why learning from the experience and the best in the IT industry is an important step in improving your online safety.

If we break it down, it doesn't mean that antivirus is dead and we should all just give up antivirus products, but rather **adopt new tools to protect against phishing attempts, spam campaigns, malicious web pages and cybercriminal attacks.**

Though you may consider for the moment that you have enough protection, future events may change your opinion. When that happens, you know you can always return to this guide and choose the best security solutions for your system.

Lesson 7 /19

Do you know about these security holes in your system?

Lesson 7

Hi there,

In the past two lessons, you've learnt about choosing the right antivirus for your computer and enhancing your security with next-generation anti-hacking tools.

But to understand how they work to protect you and why it's necessary to protect yourself from your own actions, we need to answer an essential question:

What are the dangers that threaten your data's security?

If you're like me, you surely have a bunch of gadgets you use constantly. And they're probably connected to the Internet as well (because, let's be frank, they're pretty useless without it).

How many of the devices in this list do you own?

1. Computer (laptop/desktop)
2. Smartphone
3. Tablet
4. TV
5. Kindle
6. Photo camera
7. Printer/scanner
8. MP3 player
9. Gaming console
10. GPS
11. DVD player
12. Sports bracelet
13. Headphones.

Lesson 7

Naturally, the list could do on and on, **but the key takeaway** here is that at least 7 or 8 of this list of gadgets can be Internet-connected, and, consequently, ***hackable***.

Back in 2014 (that seems like a while ago, *doesn't it?*), the **UK had more Internet-connected gadgets than PEOPLE!**

According to the numbers, the average British household owns 7.4 internet devices used to browse the web **(source)**.

Just imagine how the numbers have grown since then!

So let's get down to the nuts & bolts:

Say you have a computer, a smartphone, a tablet and a TV that are connected to the Internet through your home's Wi-fi connection.

They will be vulnerable in a number of ways against cyber criminals and their intentions:

- Your **home Wi-fi network** can be easily hacked if you don't take the necessary precautions (a dedicated guide is coming in lesson #12).

- Your **computer** can be compromised in a number of ways, both through software (malware, viruses, Trojans, etc.) and through hardware (infected USBs, for example).
- Your **smartphone** could fall prey to malvertising when browsing the web via a public Wi-fi hotspot without adequate protection.
- Your **tablet** can be compromised through malware by installing a rogue app or by visiting an infected website.
- Even **smart TVs** are vulnerable to hacking attempts, although they're not as susceptible as other gadgets. But they may be invading your privacy, by collecting your browsing data and **other confidential information** gathered through their voice recognition technology.

All these vulnerabilities (and many, many more) come from a variety of sources, and cyber criminals ace at exploiting them.

These vulnerabilities need to be managed and mitigated, so you can become aware of them and get adequate protection to the extent of your resources.

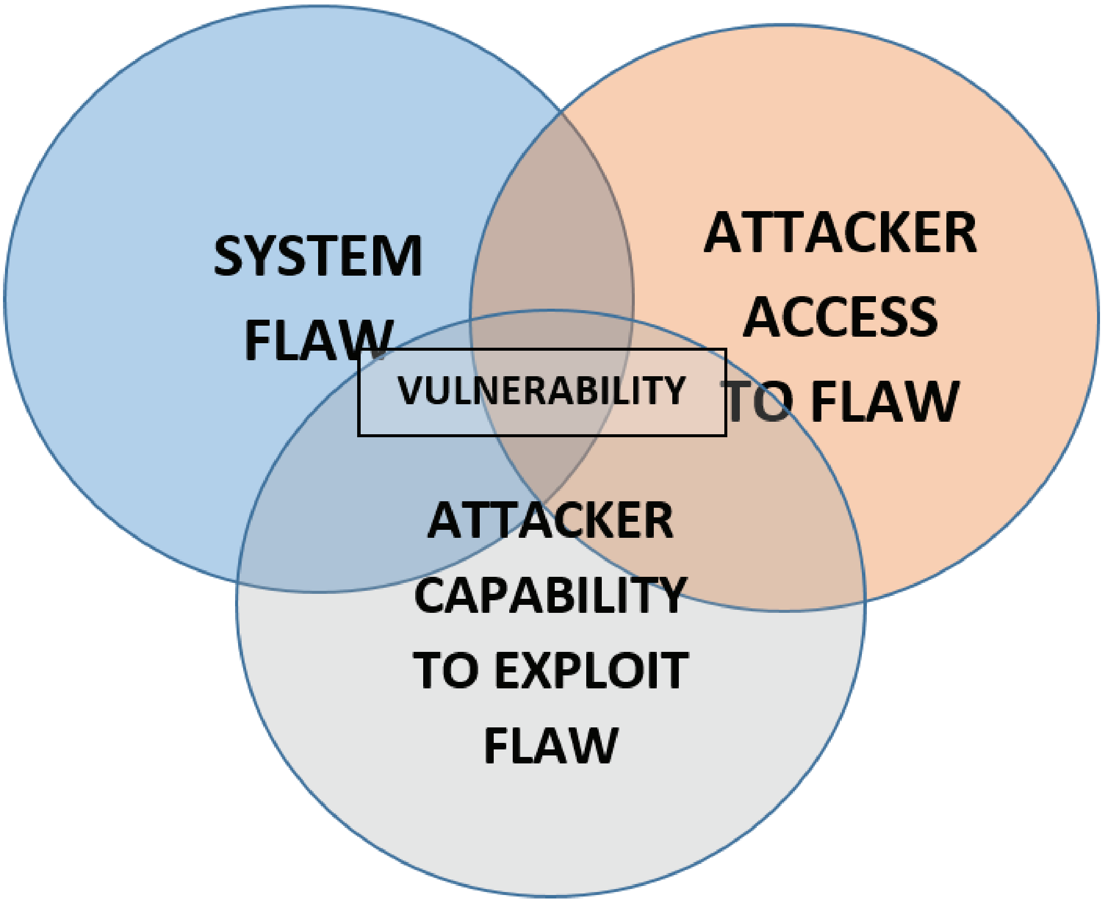
But what is a vulnerability?

A cyber security vulnerability is a weakness which allows an attacker to undermine a system's data security defenses. **It's the Achilles heel of your computer.**

Lesson 7

A vulnerability appears at the intersection of 3 elements:

1. **a system susceptibility or flaw** (example: your Java software hasn't been updated to the latest version – *seems pretty innocent, right?*)
2. **attacker access to the flaw** (example: you click on a malware-infected banner ad which delivers a download on your computer)
3. **and attacker capability to exploit the flaw** (example: now the cyber criminal has a way in, through that malicious download).



Lesson 7

Between 60% and 90% of cyber attacks are caused by a security hole in the software you use, which makes it the most used attack vector hackers employ.

So what should you watch out for?

Here is **the most vulnerable 3rd party software on the market:**

1. Oracle Java Runtime environment
2. Adobe Acrobat Reader
3. Adobe Flash Player / Plugin
4. Apple Quicktime

Of these 4, the Oracle Java Runtime Environment accounts for 180 registered vulnerabilities alone in 2013. That comes to **15 vulnerabilities PER MONTH!** The next piece of software on the list is Acrobat Reader with 66 vulnerabilities or 5.5/month, still quite high, but not as extreme.

The bad news is that you're probably using at least 3 of these types of software **right now!**

The good news is that **you can do something about it!**

Here's how you can manage your vulnerabilities:

- **Never ignore an update prompt again!** Make sure you install updates as soon as they're available or use an automatic patching software that delivers updates silently and without interrupting your work. Heimdal Free is such an option that you can **install in under 2 minutes** and which won't impact your computer's performance.

- **If you don't use it constantly, uninstall it.** Software on your computer that you rarely use most likely hasn't been updated in a long while, so it can become a security risk. Protect yourself and uninstall it.

- **Don't feed your computer junk.** The key to keeping your computer safe and performing well is not to install bad software. Unless it comes from a well-known software maker you trust, you shouldn't be installing it. The same goes for browser add-ons.

- **Use a good antivirus.** Although it doesn't offer complete protection, antivirus is essential for your system's security. Run an in depth scan once in a while – it will do nothing but good!

- **Use next-generation anti-hacking tools.** Your antivirus is a reactive solution, but you need a proactive one as well. Try to find a strong tool you can invest in that has traffic-scanning and strong anti-malware capabilities. This works proactively and strengthens your defenses substantially.

- **Keep an eye out for trouble.** Make sure to monitor any suspicious behavior on your computer. In lesson #16 you'll learn all about detecting cyber attacks and mitigating their consequences, so stay tuned.

Vulnerability management is not a practice reserved to companies, but it's also something that should become part of our routine as Internet users.

It's sort of **cyber hygiene**, if you'd like, one that it extremely necessary!

Lesson 8 /19

Stop procrastinating! Read this & Get your data to safety

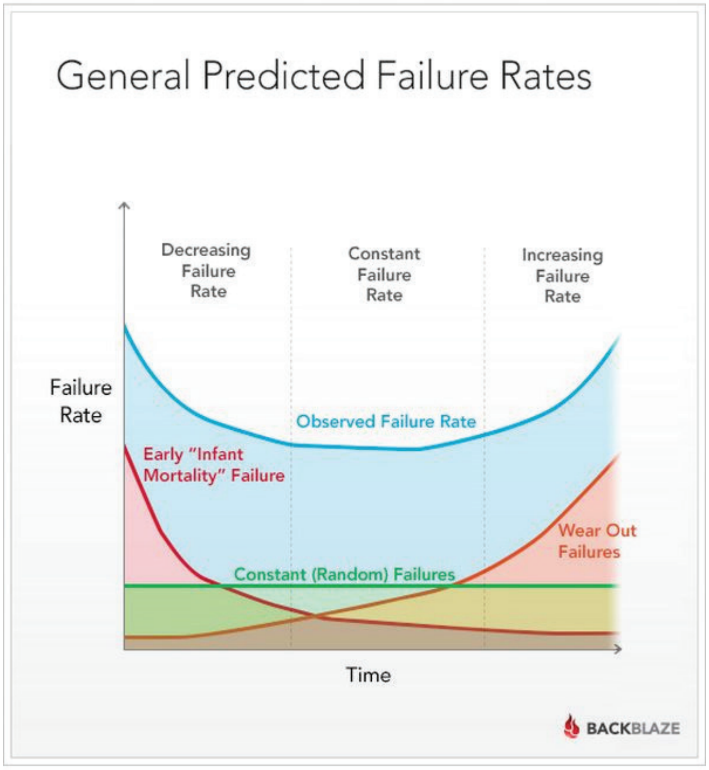
Lesson 8

In the last lesson, we talked about how to manage the vulnerabilities in your system, **so by now you're probably worried about the data on your laptop**, just like me.

And, just as I used to do, you probably keep putting off that backup you've been meaning to do for a while.

So for people like you and I, who can't really spare that much time when it comes to backing up their data, I put together this **simple, actionable guide** to stop procrastinating and get it over with.

But **if you're more the "it can't happen to me" type of person**, just take a peek below, which shows general failure rates for computer hard drives just like yours:



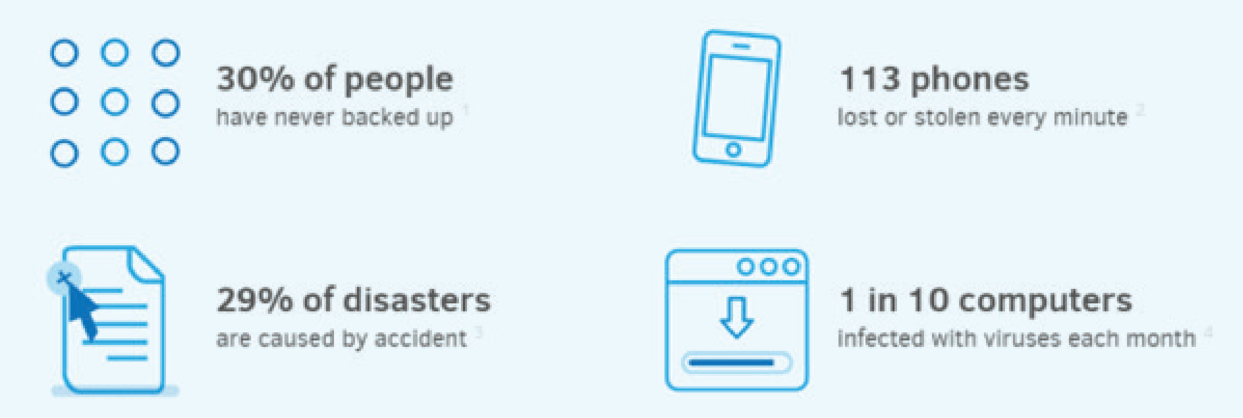
Source

*„**But who would be interested in my data?**", you may ask yourself.*

- **Cyber criminals for starters.** And they have the tools and knowledge to crack your passwords (which are probably too simple and weak, as discussed in lesson #4) in just a few minutes.

- **Real life criminals** who might steal your laptop, tablet or smartphone. Maybe they won't be interested in the data inside more than in the gadget itself, but *can you really count on that?*

- And then there are problems such as: **losing your laptop/tablet/smartphone or damaging it in some way.** You could become your own problem.



Source

*„**But backups are complicated and I don't have the skills for that!**", you might argue.*

That's a myth (and an excuse you use to justify not backing up your data). Because I know there's a lot of information out there, I created this guide to makes things simple and actionable.

Lesson 8

"I'm sure there must be some software that can recover my data, even if it gets deleted accidentally", *you may hope.*

I hate to break this to you, but NO, there isn't. There is no magic wand and no undo button for this one.

If your computer's hard drive fails, it's ALL GONE.

Could you bear losing everything on your computer: *family photos, vacation videos, work projects, financial documents, passwords, music, etc.?*

I thought so. There's only one thing left to do:

Read the steps below and apply them ASAP!

How to backup your computer: the best advice in one place

Backups are necessary copies of your data that you store somewhere safe to restore in case anything happens to the device you're working on.

For now we're going to focus on creating a backup for Windows users, but you can find a backup solution no matter what device or OS you're using. Moreover, you can also use some of the principles listed in this course to get started.

Lesson 8

Here are **2 important factors** you need to think about before starting your backup:

- *How much storage space do you need?*
- *Do you want to backup all your files or just a selection containing the most important ones?*

The 5 golden rules of data backup

1. **Keep at least 3 copies of your data.**
2. **Keep backups on different types of support.**
3. **Maintain a constant, automated backup schedule.**
4. **Keep your data backups in a secure, off-site location.**
5. **Secure your backups with strong passwords and keep those passwords safe (check the password security guide for more details).**

The rules above are simple, so now I want to help you find **the right tools** to get it done. So I have one question for you:

Lesson 8

What do you want to spend on your data's safe storage: *TIME or MONEY?*

Spending TIME

If all you want to invest is time, you can choose one of these free cloud storage services:

- **Google Drive** – 15 GB free
- **Symform** – 10 GB
- **Bitcasa** – 5 GB
- **OneDrive** – 5 GB free
- **iDrive** – 5 GB
- **Dropbox** – 2 GB (you can win up to 16 GB of free space through referrals)
- **SpiderOak** – 2 GB
- **Google Photos** - unlimited, high-quality photos and videos.

If the stuff you want to backup fit in the free space offered by one of these services, all you have to do is couple it with a free backup software and you're done! And we have just the list for you: **34 Free Backup Software Tools.**

Spending MONEY

If your backup needs exceed these free options, you should keep in mind that **online backup software and storage is not expensive!**

Let me give you some examples:

Cloud storage (pricing per month):

- Google Drive – $1.99 for 100 GB or $9.99 for 1 TB (check out **the rest of the options**)
- OneDrive – $1.99 for 100 GB or $6.99 for 1 TB, including
- Office 365 (check out **the rest of the options**)
- Dropbox – $9.99 for 1 TB or $15 / user / month for unlimited(!) storage **(details)**
- SugarSync – $7.49 for 100 GB or $9.99 for 200 GB (check out **the rest of the options**)
- Symform – $10 for 100 GB or $20 for 200 GB (check out **the rest of the options**)
- Bitcasa – $10 for 1 TB or $99 for 10 TB **(details)**
- SpiderOak – $12 for 1 TB **(details)**.
- Amazon Cloud Drive – $11.99/year for storing unlimited photos or $60/year for unlimited everything **(details)**.

Online backup services (pricing per year):

- iDrive – $45 **(details)**
- BackBlaze – $50 **(details)**
- CrashPlan – $60 **(details)**
- Carbonite: $60 **(details)**
- Acronis: $100 **(details)**
- O&O Disk Image 9: $50 **(details)**
- Rebit 6: $40 – one time payment **(details)**.

You can also this **great comparison tool** to evaluate features and pricing for multiple software options. Check out the homepage on **BestBackups.com** as well for backup tools for other operating systems and focused on specific criteria.

Because you should follow backup rule nr. 2 – **keep backups on different types of support** – let's check some **external drives options** as well:

- HGST Touro S 1TB – $70 **(details)**
- HGST Touro Mobile 1TB – $55 **(details)**
- Seagate Expansion 1TB Portable – $65 **(details)**
- Seagate Backup Plus Slim 1TB – $65 **(details)**
- Seagate Expansion 1TB – $60 **(details)**
- Toshiba 1TB Canvio Basics – $58 **(details)**.

All that you have to do now is:

1. Make a choice of a free or paid storage
2. Pick a backup software solution
3. Choose the files you want to back up
4. Set a constant backup schedule
5. Sit back and know that your data is safe.

That wasn't as difficult as you imagined, now was it?

Now that you've put your data to safety, let's see why you need data encryption (even if you're not a security specialist). **Coming up in lesson #9!**

Lesson 9 /19

You need data encryption (even if you're not a security specialist)

Lesson 9

Our last guides provided useful instructions on how you can select the best security products and what backup solutions you can use for the protection of your system files.

You can't really build a decent security strategy without using a few reliable **encryption mechanisms** that are able to secure our essential data from online threats and privacy breaches.

But what exactly is data encryption?

Encryption is a process that transforms accessible data or information into an unintelligible code that cannot be read or understood by normal means.

The purpose of encryption is to secure sensitive information from cyber-criminals or other online dangers. At the same time, it is a method that can be used to archive large amounts of data or secure private communication over the Internet.

Encryption tools are very useful in keeping valuable information hidden from hackers and you should use some sort of encryption every time you access personal information, no matter it is used in local operations or sent over the Internet.

9 Free Encryption Software Tools to Protect Your Data

There are many encryption tools that can protect your valuable information from data breaches and online criminals, but I have selected **9 free tools** that can be used fast to protect your data.

Use strong passwords for your online accounts

Encrypting files is not so helpful if you don't pay attention to the password you set to access your encrypting programs, because your encryption is only as good as your passwords.

1. LastPass

To protect your passwords and increase your online safety, I recommend a password manager as LastPass. Using this password manager, you'll only need to remember one password, the one that you use to access LastPass.

LastPass provides extensions for the main web browsers, like Mozilla Firefox, Internet Explorer and Google Chrome.

When you access a new online account, it immediately offers you the option to save the new credentials and encourages you to set a unique and hard to break password for only one account. If you are using the same password in multiple locations, it simply recommends selecting a different password.

*Remember **lesson 4?*** I hope you've already applied the steps there, so that you can check this off and move on to the next thing!

Encrypt Your Hard Drive

2. BitLocker

There are a number of encryption tools that you can use to protect your operating systems and our files from any online danger.

But the easiest way to encrypt sensitive information or maybe the entire hard-disk is to use Microsoft's BitLocker software, which is now installed on most Windows operating systems.

What exactly is BitLocker?

BitLocker is a full-disk encryption tool incorporated in the latest Windows operating systems, which supports AES (128 and 256-bit) encryption and it's mainly used to encrypt the entire hard disk.

What is the AES encryption used by most security software?

The Advanced Encryption Standard has been tested and improved and is now used worldwide by most security vendors due to its high level of security and optimization.

Why am I recommending this tool?

I simply recommend this tool because it is easy to use and it is already accessible to many people that use the Windows operating system.

BitLocker Drive Encryption is mainly a tool we can use to prevent access breaches to any file from our hard-disk. That's because BitLocker encrypts the entire drive, which makes it impossible for anyone stealing your laptop to remove the hard drive and read the files.

3. VeraCrypt

VeraCrypt is free and it is available for Windows, OS X and Linux operating systems. If you are used to TrueCrypt, then you will have no problem in using VeraCrypt, which supports Advanced Encryption Standard and can hide encrypted volumes within other volumes.

Though some people are still using TrueCrypt, I recommend that you go for VeraCrypt because this tool is under development and security updates are delivered for its improvement.

Though VeraCrypt does not support TrueCrypt files, you can convert them to its own format.

Encrypt Your Files

4. 7Zip

There are many users that don't want to encypt the entire hard disk, but only files and documents that contain valuable data or information that needs to be sent over the Internet.

7Zip is powerful and lightweight solution that is great by its simplicity. As many users noticed, 7Zip is capable of extracting most archives, the program is easy to use for encrypting your own files and it uses one of the best compression formats.

5. AxCrypt

Like 7Zip, AxCrypt is a lightweight free encryption tool that integrates with Windows and you can use it mainly for protecting valuable files from the system.

The files can be encrypted for a specific period of time and can auto-decrypt later on, when that file reaches the destination. It is a fast tool that enables the user to select an entire folder or a group of files and encrypt them fast.

As I mentioned at the beginning, its main purpose is to be used for protecting files and not entire hard drives, though it does offer protection against major cracking methods used by hackers.

Encrypt your Online Traffic

Encryption for private files is not enough. **To increase overall protection, you need to make sure your communication is not easily accessed by hackers or malicious software.**

So, how do you increase online security without creating too many barriers that may slow us down between our computers and the content you want to access?

I have considered below a few simple tools you can use to access online content and stay safe from privacy breaches at the same time.

6. Access secure websites that use encryption mechanisms

To make sure you always access secure web pages, you can use a browser extension like **HTTPS Everywhere**, which works on Mozilla Firefox, Opera and Google Chrome.

Though some security analysts argue that even on secure websites a user is not completely safe, it is better than nothing. After all, these secure websites use some encryption and authentication standards that are meant to protect confidentiality of online activities.

In this case, for example, when your browser connects to a secure website, there is an authentication process which uses cryptography to verify that a secure connection is maintained.

For this reason, using a little extension like HTTPS Everywhere that encrypts your communication with major websites makes your online presence more secure and safe from cyber-crime.

7. Tor Browser – Access the Anonymity Network

What If I Want Complete Protection Online?

If you want complete privacy, you can use the Tor browser, which allows you to access Internet anonymously using the Tor network of computers.

The special **Tor browser** has been designed to be used by anyone who wants to hide any browsing activity from prying eyes.

But, what exactly is Tor?

Tor is the short version of **"The Onion Router"** and it is the browser that you download on the system, but also the Tor network of computers that manage the connections and route the traffic.

By routing the online communication through multiple systems in the Tor network, it is almost impossible for any interested party to trace the traffic communication back to the origin.

Finally, the number of computers in the network become a highly effective layer of protection that conceals the user identity.

You may have heard already about cases where Tor anonymity network has been used for malicious purposes.

I understand that you may see some connections between online browsing and criminal activities, but as Tor network representatives mention, they simply give normal individuals the same privacy privileges that cyber-criminals are already able to access.

8. Virtual Private Network – Encrypt Your Communication

Are there alternatives for becoming anonymous online?

Lesson 9

Yes, to connect in complete privacy to any online location in the world, you can use a VPN, which is a Virtual Private Network.

This private network is able to spread across the normal Internet space, using its resources to create an encrypted channel that can keep your communication safe from intercepting attempts.

Usually, a VPN is used by remote workers to access the private company network and run online operations or transfer highly confidential documents in complete privacy.

Therefore, using a VPN software, you can make sure that your web traffic and your valuable information remain encrypted and cyber-criminals are prevented from sniffing the data you exchange online.

But, VPN software is not just for corporate users, such a software can also be used by a normal user when connecting from unsafe public networks or when they want to access censored content.

To keep your online session private over the Internet, I recommend a popular **VPN** solution like **CyberGhost**.

Lesson 9

9. Online Proxy Server – Hide Your IP Address

If you don't want to go through all the hassle of finding and installing a **VPN software or the Tor browser** and be suspected by your friends that you're running some suspicious dark net activities on some underground market, I still recommend a basic privacy measure, such as an online proxy server.

Using a proxy server, you can simply hide your IP address and surf online accessing websites anonymously.

Though a web proxy server cannot offer the encryption channel you obtain from a VPN solution and is not able to hide your online communication through an entire network like Tor, you still have an indirect link between your computer and the website you access, which is enough protection for small size browsing activities on blocked or censored web pages.

Encryption is not enough (either)

To keep your valuable information safe from cyber-criminals, encryption is not enough. No one single tool can provide you with the complete protection you expect.

Lesson 9

The hackers' arsenal contains a lot of software weapons that you need to shield your systems from. Since there are so many dangers online, I would like to recommend a few easy steps you can take to stay safe over the Internet.

- **Keep your browser and your operating system updated with the latest security patches.** Make sure you have the latest programs and applications on your system. Online criminals spread malicious tools by using security exploits to take advantage from your system's vulnerabilities.

- **Use a reliable security program from a big company.** To keep your system safe from the latest threats, the software should include a real-time scanning engine, which means that everything that you download is scanned. We have dedicated lesson 6 to this topic.

- **Be careful when connecting to** public **and free wireless networks.** One of the favorite methods used by online criminals to retrieve your credentials is by using wireless sniffers to access data sent over unprotected networks. As promised, in **lesson 11** I'll do a complete walk-through in Wi-Fi networks protection.

Lesson 9

When you think about encryption, you need to set in place not only a security strategy for your private computers, but ways to make sure personal information doesn't leave your computers while you go online.

For this reason, encryption should be applied not only to sensitive files and documents from the local disk, but to our online traffic, since in that environment are now hidden the greatest threats.

Here's what you can do right now:

Test the solutions that protect your Internet traffic and check if any of them affect your online speed. If you are OK with them, keep them further to maintain your online privacy.

Lesson 10 /19

And the cyber security specialists said secure thy browsers or...

Lesson 10

Hi there,

In our previous guide, I presented 9 tools that you can use to encrypt your files and your online traffic, but before you start using additional means, ***shouldn't you try first to improve your online safety by increasing your browsers' security settings?***

Today, some of the most popular web browsers, like **Internet Explorer, Mozilla Firefox** and **Google Chrome** are installed on most Windows operating systems. For this reason, these 3 web browsers are the most important tools most of us use for going online.

How your browsers are exposing you to cyber attacks
Before you can configure your browser and increase your online security, you need to understand a few terms since you will have to deal with them again frequently.

The features presented below are important for your browser's operation and for your online security, therefore we must acknowledge their role before we can decide if we need to disable them or not.

- **ActiveX** is a software component or an add-on of Windows operating systems and it is required by some websites to view certain elements or take actions, improving the general browsing experience. At the same time, online criminals use ActiveX in creating and adding malicious ActiveX software to web pages in order to damage computers.

- **Java** is a programming language developed to create applications on our computers or active content on a website. Java has two parts: the

Java application that runs on our computers and the browser plug-in, which we recommend you to disable unless you really use it.
The Java browser plug-in opens up a great number of security holes allowing hackers to access your personal data.

- **JavaScript** is a programming language that makes web pages interactive and is used mainly for displaying dynamic content, improving your online experience. The problem with JavaScript is that many viruses are script based and a great number of scripts can be dangerous being used to perform a number of malicious tasks.

- **Cookies** are files which are stored on your browser and hold some amount of data about your browsing history. They can be accessed by a website in order to improve your browsing session, though this behavior has given rise to privacy concerns and security issues.

- **Extensions** or **add-ons** are pieces of software that add or modify a feature or a functionality in your web browser. Some of them allow you to block ads, watch online videos or they are closely integrated in social media websites improving your online session. The possible issues which may appear from extensions is that some of them can be used to inject ads into the sites you visit or track your entire browsing activity.

Secure your web browsers: Internet Explorer, Mozilla Firefox, Google Chrome

You probably didn't know this, but there is a right way to configure your browser and there's a wrong way. It is a necessary step we need to take, because our web browser is not setup for the best security in the default configuration.

If you choose not to take any action to secure your browser, you may allow anything on our computers, from malicious software applications to online criminals that are more than prepared to take advantage of our weaknesses.

Though we cannot guarantee complete safety from malware attempts and online attacks, we know that following the steps below will increase your web browser security. At the same time, we cannot name one single browser as the best possible selection for a user, since so many studies and articles name one over the other.

For this reason, we will simply choose to present the 3 most popular web browsers for Windows: **Google Chrome, Internet Explorer and Mozilla Firefox**.

Internet Explorer (jump to section)

Mozilla Firefox (jump to section)

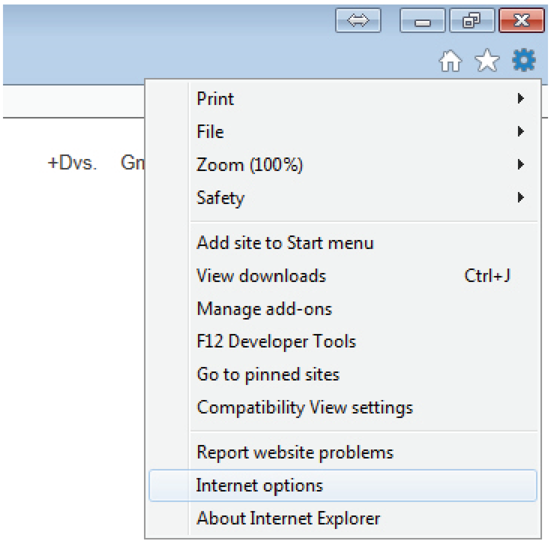
Google Chrome (jump to section)

Internet Explorer

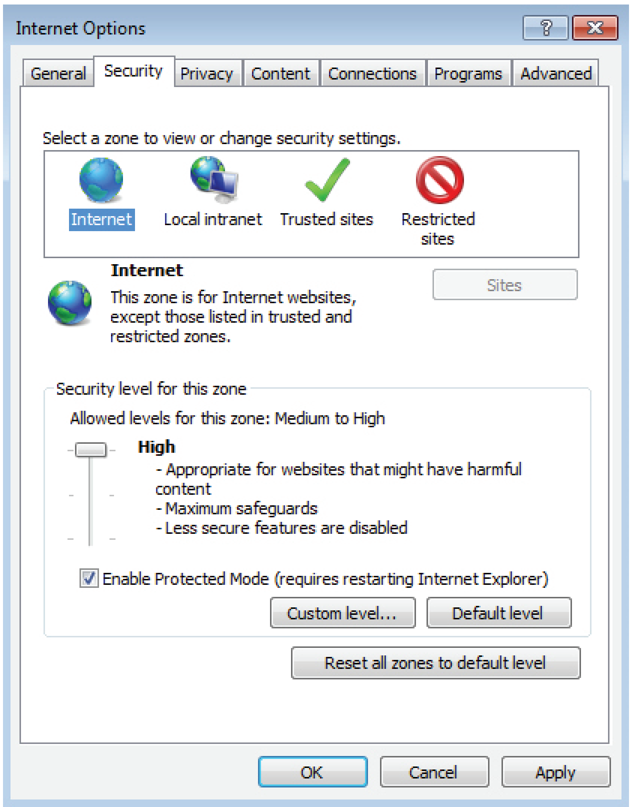
Microsoft Internet Explorer is one of the most popular web browsers in the world. And it is quite normal, since it arrives already integrated in our Windows operating systems. It supports Java and other active content, and it also implements ActiveX technology.

To improve your overall security configuration in Windows 10, you need to access your browser settings area. Please make the necessary changes in case you are using a different version of Internet Explorer.

To improve your **Internet Explorer settings**, access the **Internet Options** area:



Go to the **Security** tab from the top menu.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Sites

Security level for this zone

Allowed levels for this zone: Medium to High

High

- Appropriate for websites that might have harmful content
- Maximum safeguards
- Less secure features are disabled

☑ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

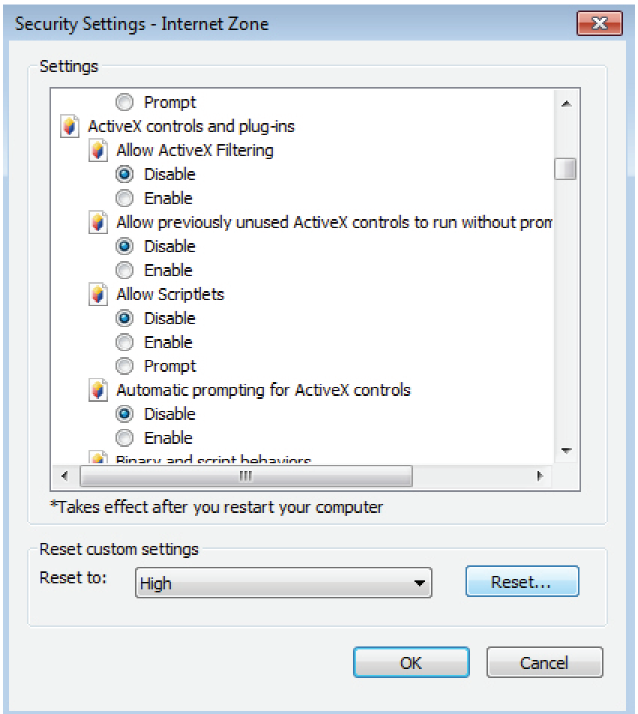
In this area you will find multiple security zones for your computer and you also have the possibility to customize each security zone.

1. **Increase Your Security Level**
   For the Internet zone we recommend you to select the **High security level**. This selection will disable some browser features, such as ActiveX, Active scripting and Java, which acted sometimes as security breaches and even open gates for online threats.

Lesson 10

2. Customize the Security Level

To customize the security settings for a zone, choose the **Custom Level** option.



Security Settings - Internet Zone

Settings

○ Prompt
ActiveX controls and plug-ins
Allow ActiveX Filtering
● Disable
○ Enable
Allow previously unused ActiveX controls to run without prom
● Disable
○ Enable
Allow Scriptlets
● Disable
○ Enable
○ Prompt
Automatic prompting for ActiveX controls
● Disable
○ Enable
Binary and script behaviors

*Takes effect after you restart your computer

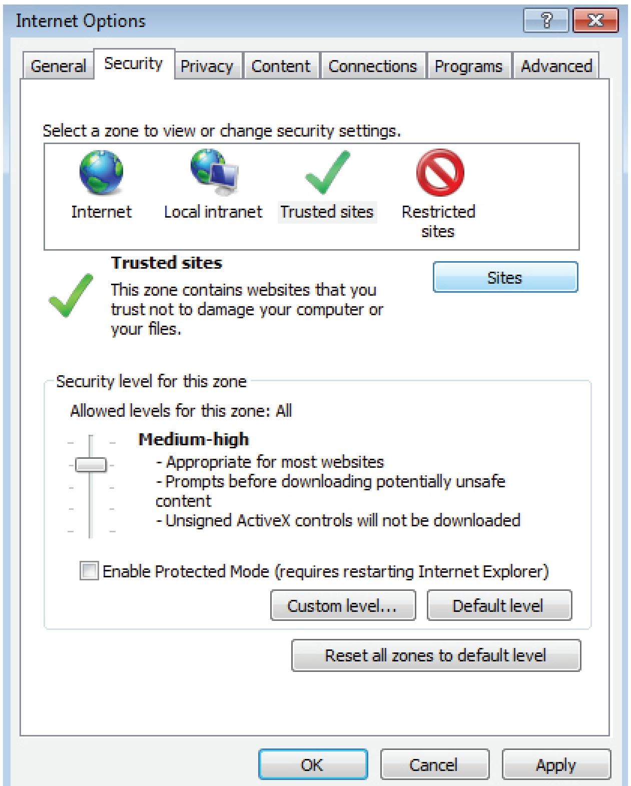
Reset custom settings

Reset to: High

In this area you can enable or disable specific security options for your selected Internet area. To return to the default levels for the selected Internet zone, simply click the **Reset**... button available.

3. Add a website to the Trusted Sites List

If we return to the initial window and click the **Trusted sites** option, we find a security zone for sites which are safe to access.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Sites

Security level for this zone

Allowed levels for this zone: All

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

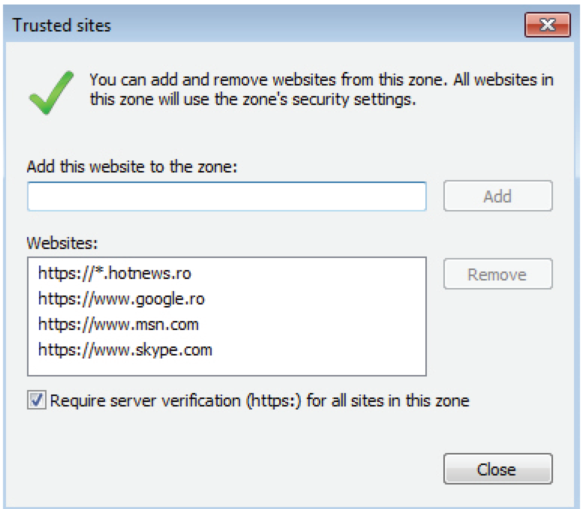
□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

If you consider a particular website to be a safe online location that can be trusted, you can choose to add it to this area. To do this, click **Sites**.



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

Websites:

https://*.hotnews.ro
https://www.google.ro
https://www.msn.com
https://www.skype.com

Remove

☑ Require server verification (https:) for all sites in this zone

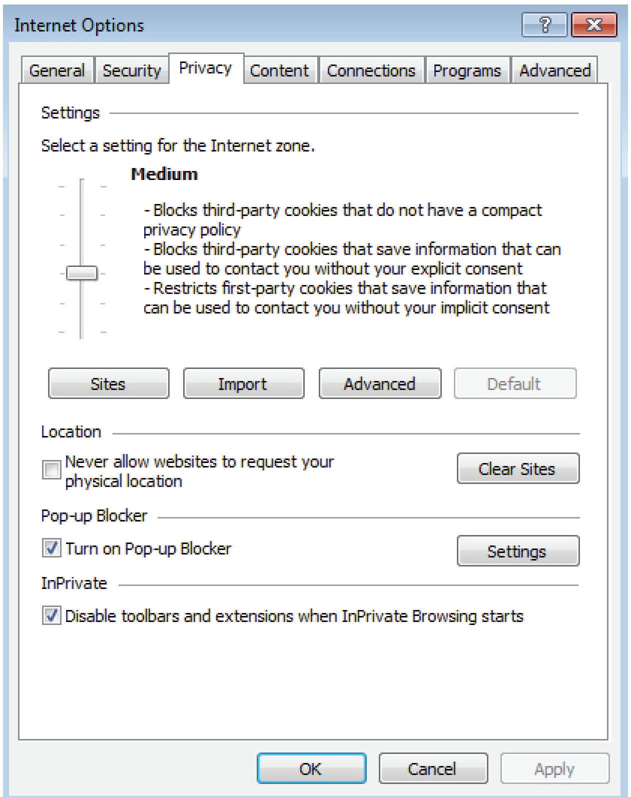
Close

In this area you can choose to add the website to a list of safe web locations. You can also choose to remove a site from the list.

The **Trusted sites** zone is useful if you chose the **High** security level for the Internet zone. Setting the High security level in the Internet zone causes browser features like **ActiveX and Active scripting** to stop functioning, and you may encounter some websites that don't function normally after that.

To solve this, simply go to the **Trusted sites** zone and add the site that doesn't function as it should. Adding the site to the Trusted sites zone means that the website will work normally, by loading the browser features that are not allowed to function in the High security level.

4. **Privacy Settings**
   The **Privacy** tab contains various settings for cookies in Internet Explorer.


Internet Options
General | Security | Privacy | Content | Connections | Programs | Advanced
Sites
Import
Advanced
Default
Clear Sites
Settings
OK
Cancel
Apply

Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Location

□ Never allow websites to request your physical location

Pop-up Blocker

☑ Turn on Pop-up Blocker

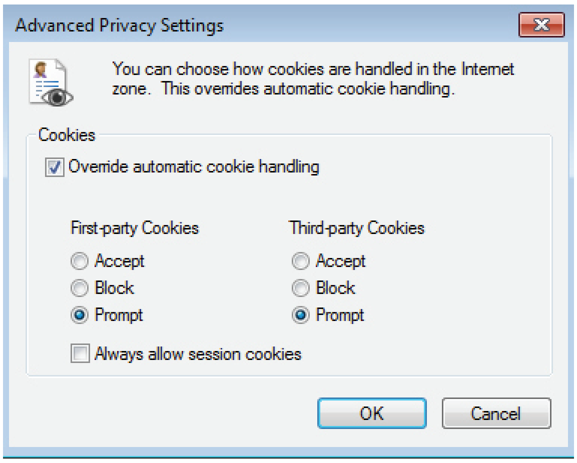
InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Cookies are text files that are placed in your computer by websites you access. They contain data and information the sites store about your browsing habits or your preferences. In this space you can use the pre-set privacy rules available by using the slider and select one of the settings for your Internet zone. For example, choosing the High level will block cookies from most websites.

If you want to make modifications, you have other additional options.

To improve your security, select the **Advanced** button available.



You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

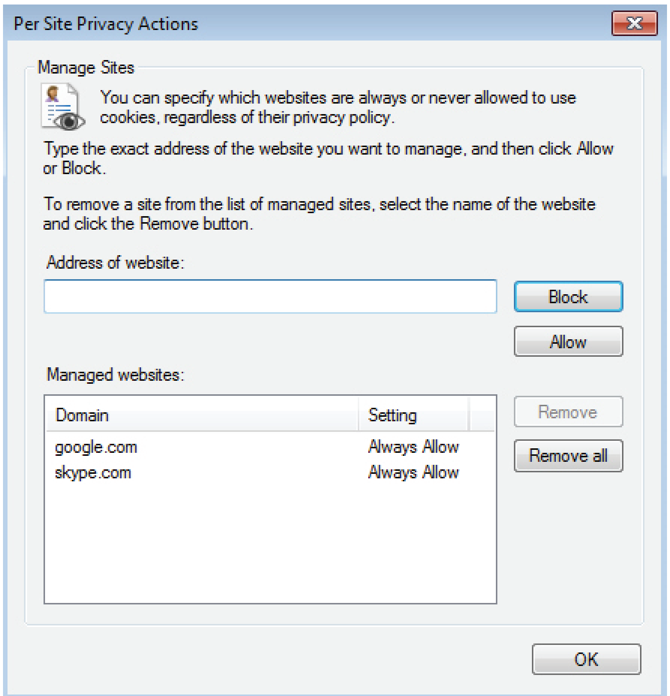
First-party Cookies
○ Accept
○ Block
● Prompt

Third-party Cookies
○ Accept
○ Block
● Prompt

□ Always allow session cookies

In this area, check the **Override automatic cookie handling** option and select **Prompt** for both first and third-party cookies. You will be asked each time a website tries to place a cookie on your computer. For example, if you visit an online shop associated with advertising, you may choose to block the cookie in order to prevent the website from sending you ads and affect your privacy.

If we go back to the **Privacy** tab and select the **Sites...** button, we have the option to manage cookies for a specific website.



You can specify which websites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the website you want to manage, and then click Allow or Block.

To remove a site from the list of managed sites, select the name of the website and click the Remove button.

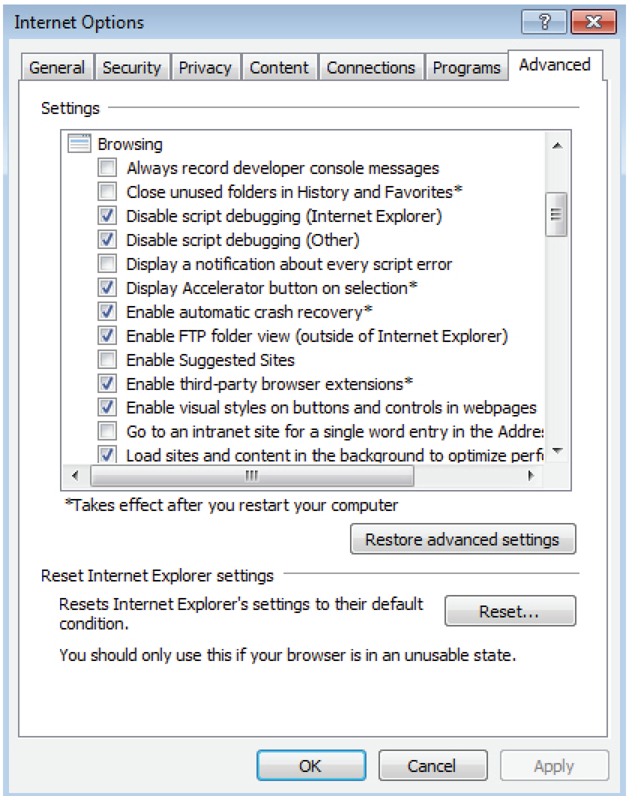
Address of website:

Domain	Setting
google.com	Always Allow
skype.com	Always Allow

In this area, you can choose to allow or block cookies from a particular website.

A last security step we recommend you to take in Internet Explorer is in the **Advanced** tab.

Lesson 10



Internet Options

Settings

Browsing

- ☐ Always record developer console messages
- ☐ Close unused folders in History and Favorites*
- ☑ Disable script debugging (Internet Explorer)
- ☑ Disable script debugging (Other)
- ☐ Display a notification about every script error
- ☑ Display Accelerator button on selection*
- ☑ Enable automatic crash recovery*
- ☑ Enable FTP folder view (outside of Internet Explorer)
- ☐ Enable Suggested Sites
- ☑ Enable third-party browser extensions*
- ☑ Enable visual styles on buttons and controls in webpages
- ☐ Go to an intranet site for a single word entry in the Addre
- ☑ Load sites and content in the background to optimize perf

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

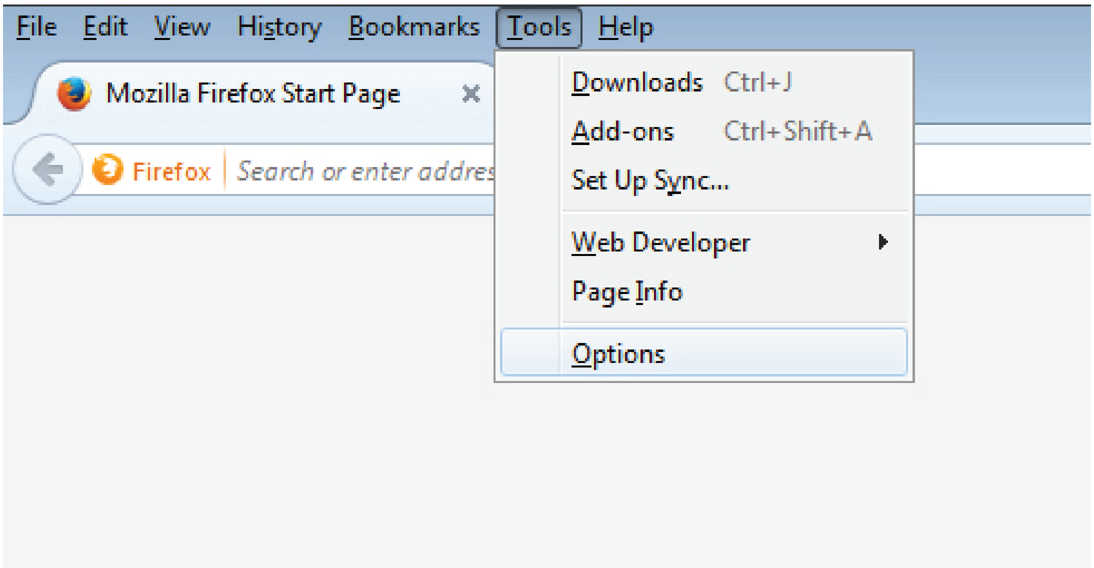
This area contains settings that apply to all security zones. From this tab, we recommend you to uncheck **Enable third-party browser extensions** option. If you leave it checked, different type of toolbars and add-ons are enabled on your system and this may affect your privacy. Many add-ons have proved to monitor your browsing habits or even attempt to collect private data from your browser.

Mozilla Firefox

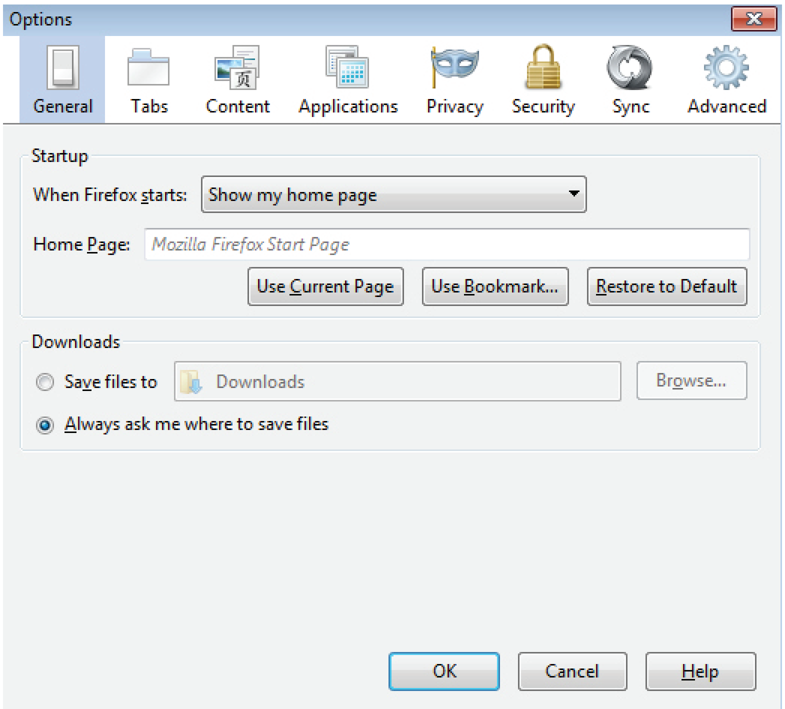
Mozilla Firefox is another popular web browser and there are a few steps we can take to improve its security settings.

To increase your protection against online threats in Mozilla Firefox (version 32.0.2), you need to access the settings area. Please make the necessary changes in case you are using a different version of Mozilla Firefox.

To access the settings area for Mozilla Firefox, select **Tools** and **Options**.



In the **Options** window, you need to access first of all the **General** category from the top menu.



Startup

When Firefox starts: Show my home page

Home Page: Mozilla Firefox Start Page

Downloads

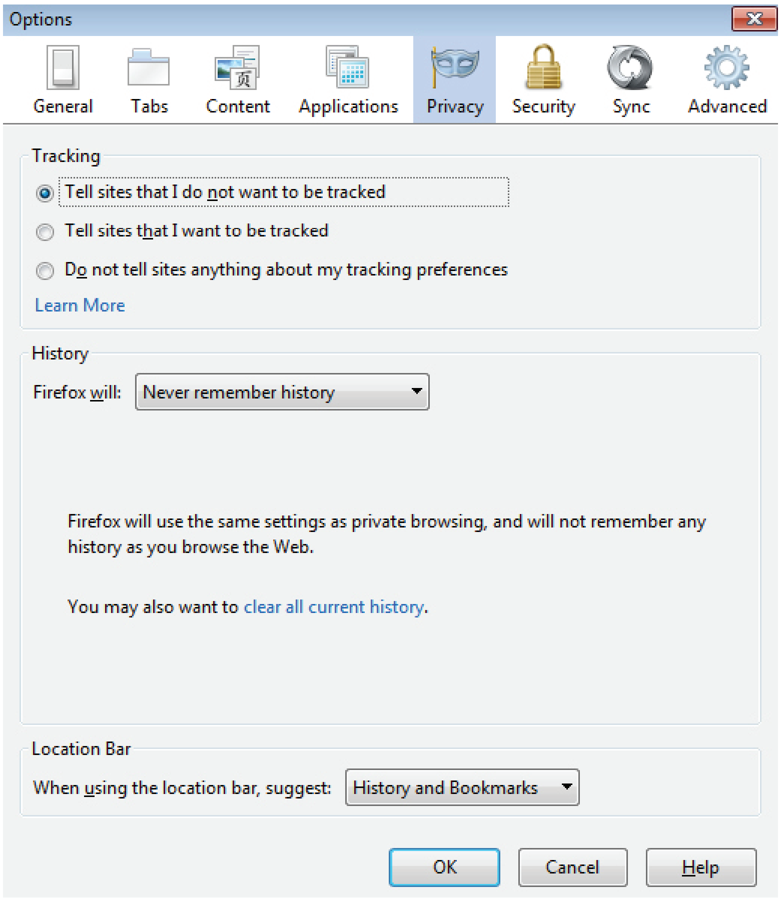
○ Save files to Downloads

● Always ask me where to save files

1. **Automatic download**
   Under this section, you can select the option **Always ask me where to save files**. This way, you won't have a web location trying to automatically save dangerous content to your computer. At the same time, you have the option to place suspicious content in a location where you can analyze it afterwards.

2. **Tracking Settings**
   The next step is to access the **Privacy** category, where you find the **Tracking** and **History** sections.

Lesson 10



Tracking

● Tell sites that I do not want to be tracked

○ Tell sites that I want to be tracked

○ Do not tell sites anything about my tracking preferences

Learn More

History

Firefox will: Never remember history

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

Location Bar

When using the location bar, suggest: History and Bookmarks

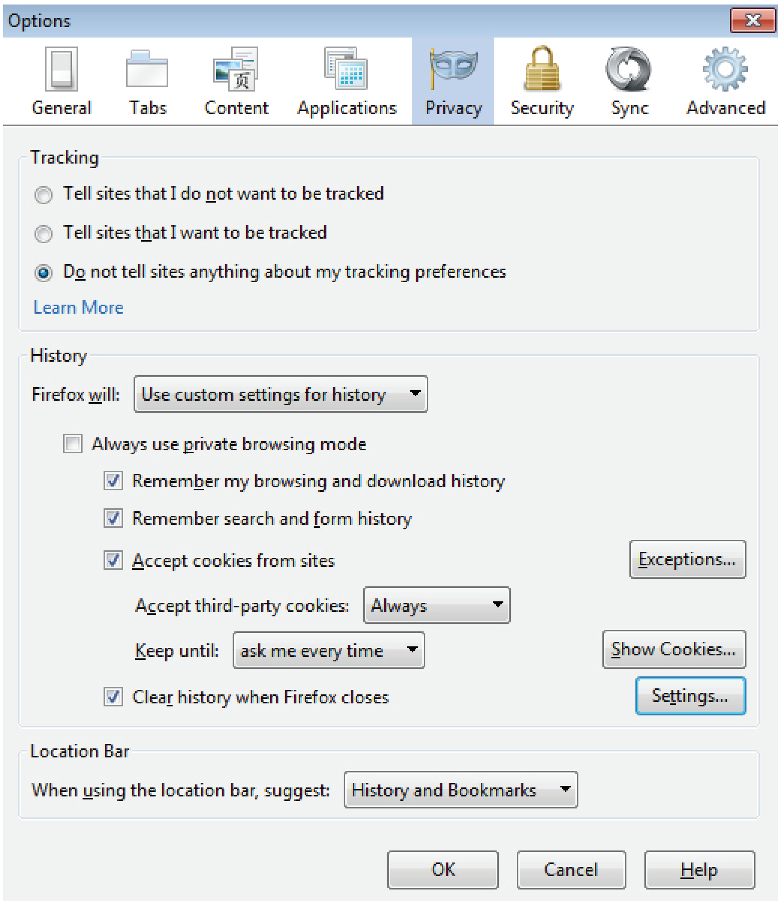
In the **Tracking** section, check **Tell sites that I do not want to be tracked**. Selecting this option informs a website that you would like to opt-out of third-party tracking for advertising purposes.

3. Privacy Settings

In the History section, choose your browser **Never remember history**, especially if you are using a computer from a public location or you know that computer is used by more people.

Lesson 10

For a more detailed configuration of your **History** section, select from the drop-down menu **Use custom settings for history.**



Tracking

○ Tell sites that I do not want to be tracked

○ Tell sites that I want to be tracked

● Do not tell sites anything about my tracking preferences

Learn More

History

Firefox will: Use custom settings for history

□ Always use private browsing mode

☑ Remember my browsing and download history

☑ Remember search and form history

☑ Accept cookies from sites

Accept third-party cookies: Always

Keep until: ask me every time

☑ Clear history when Firefox closes

Location Bar

When using the location bar, suggest: History and Bookmarks

4. Private Browsing Mode

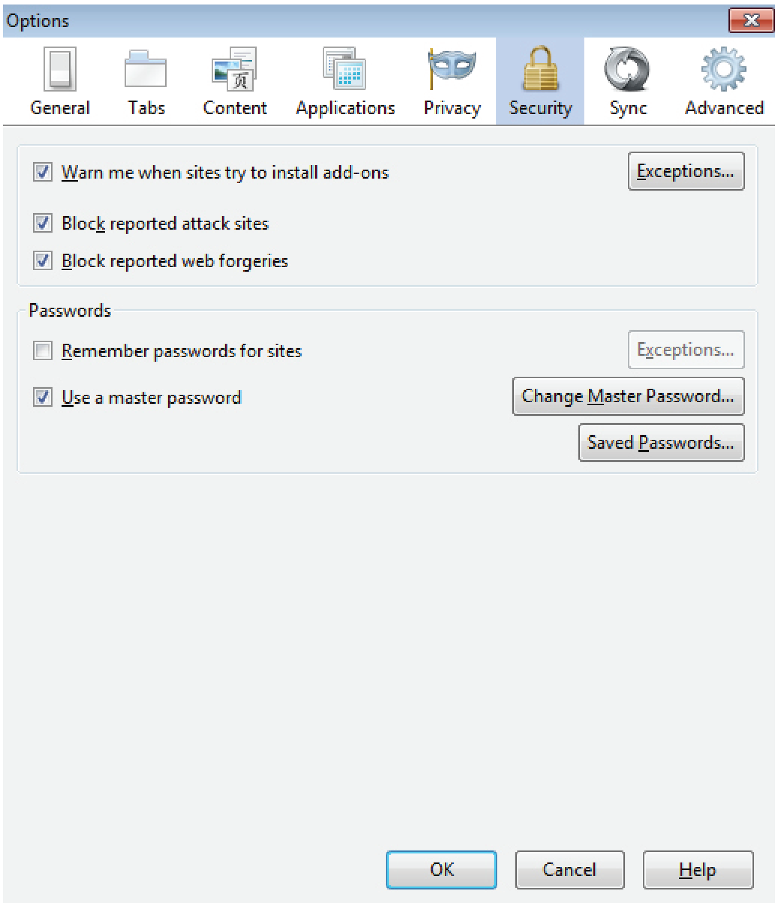
You can also select **Always use private browsing mode**, which we highly recommend if you find yourself in a shared environment. Selecting this option ensures that when you finish your Mozilla Firefox session, all browsing, search and download history, and all the cookies are removed.

Lesson 10

For a more detailed configuration of your online browsing settings, choose from the available options.

5. Malware and phishing protection

The last changes we need to make are in the **Security** category.



☑ Warn me when sites try to install add-ons

☑ Block reported attack sites

☑ Block reported web forgeries

Passwords

□ Remember passwords for sites

☑ Use a master password

First of all, make sure that the first 3 options **Warn me when sites try to install add-ons, Block reported attack sites** and **Block reported web forgeries** are all checked. In case a site tries to install an add-on, you will see a warning at the top of the browser about this.

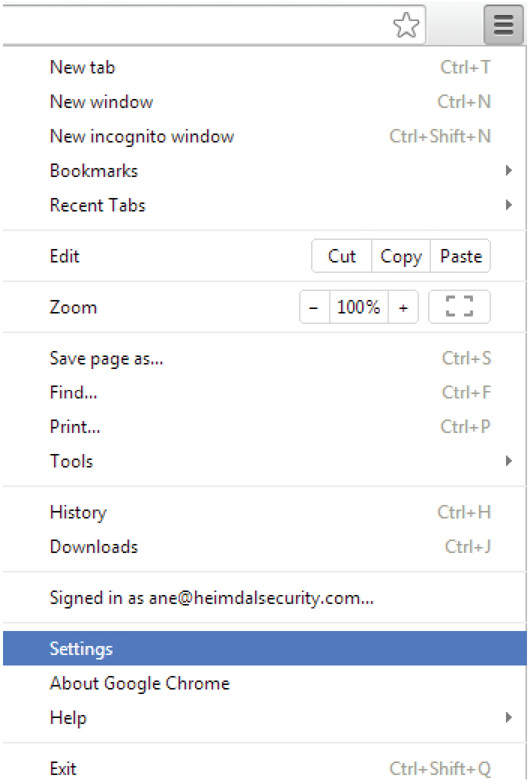
6. **Passwords Security**
   Further on, the **Passwords** section contains various options to store and manage your passwords and we recommend you to use this option if you let Mozilla Firefox take care of your credentials. In the same location you can find a Master Password feature, which helps you encrypt data on the system.

Google Chrome

Google Chrome is a web browser used by more and more people in the last years and there are a few actions we can also take here to increase our online security.

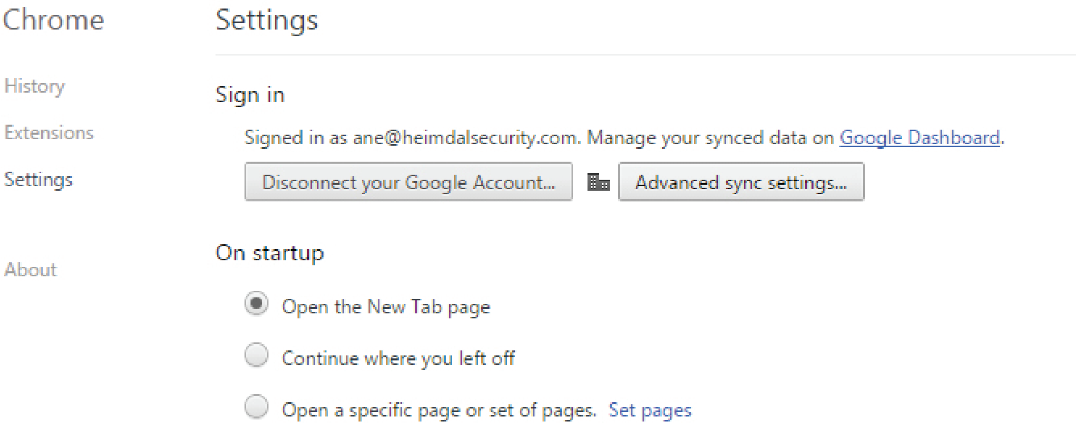
To start making the necessary modifications, we need to access the **Settings** area. Again, please make the necessary changes in case you are using a different version of Google Chrome.

To access the settings area for Google Chrome, click the available button at the top right corner of the browser and select **Settings** from the drop-down menu.



1. (Don't) Sync your Google Account

As soon as you access the **Settings** area, you will notice at the top, in the **Sign-in** section, **Advanced sync settings...**



Sign in

Signed in as ane@heimdalsecurity.com. Manage your synced data on Google Dashboard.

Disconnect your Google Account... | Advanced sync settings...

On startup

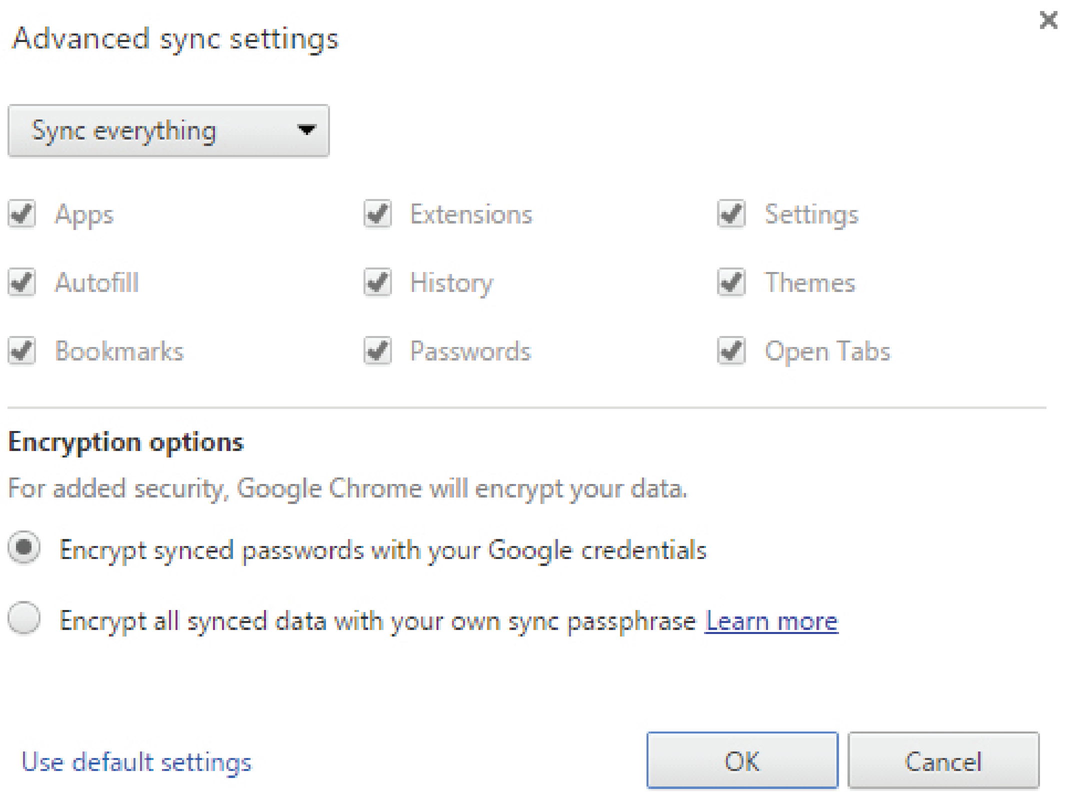
● Open the New Tab page

○ Continue where you left off

○ Open a specific page or set of pages. Set pages

Lesson 10

Google Chrome gives you the possibility to sync your settings and data with other systems or mobile devices where you signed-in with your Google account. This creates a vulnerability risk, since you are required by default to connect **with only your Google account** on a device that syncs with your other systems or devices (where you have added your Google account).



Advanced sync settings

Sync everything

☑ Apps ☑ Extensions ☑ Settings

☑ Autofill ☑ History ☑ Themes

☑ Bookmarks ☑ Passwords ☑ Open Tabs

Encryption options

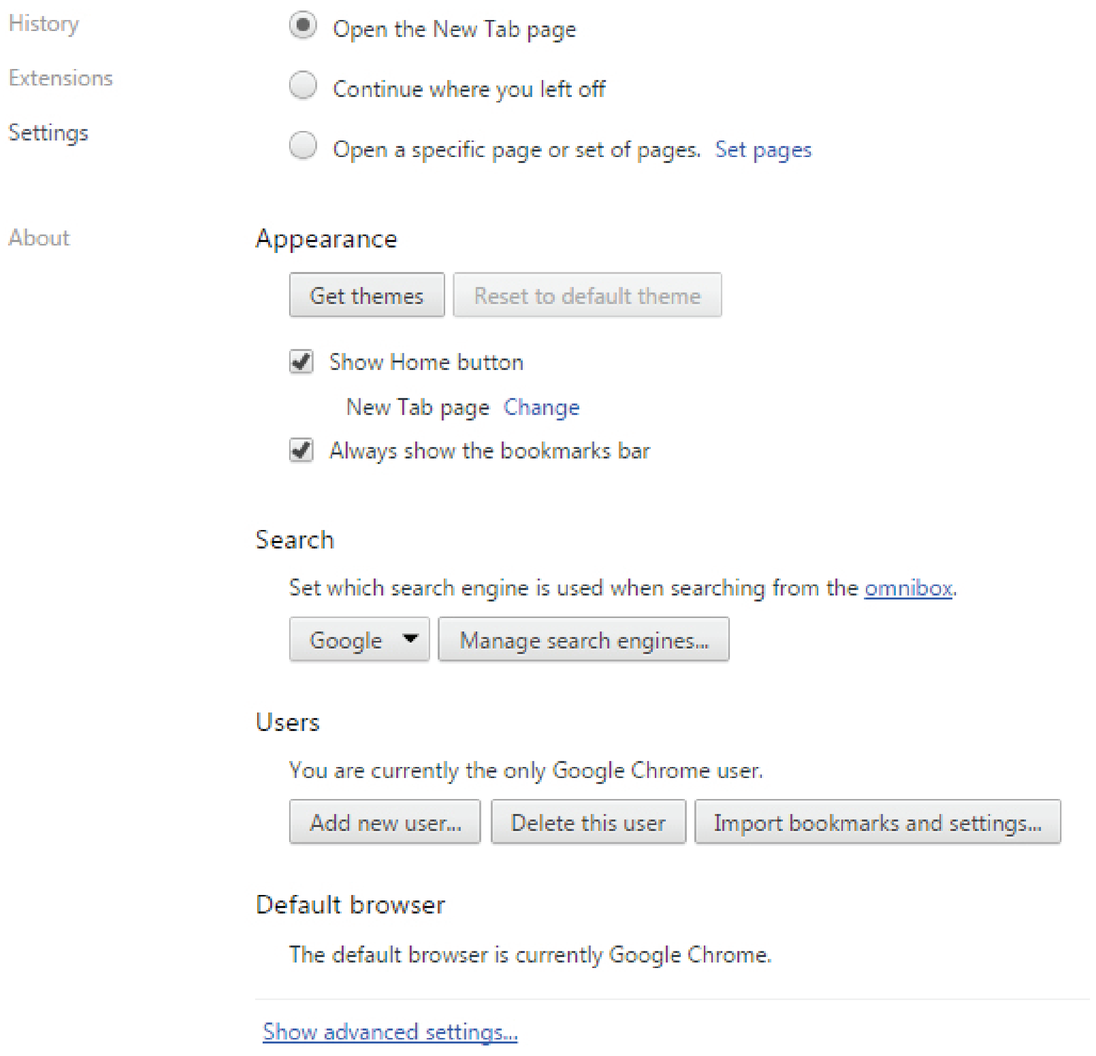
For added security, Google Chrome will encrypt your data.

● Encrypt synced passwords with your Google credentials

○ Encrypt all synced data with your own sync passphrase Learn more

To improve your security, you need to **set a passphrase,** which is an additional credential required to sync your devices.

If you scroll down at the bottom of the page, you will see a Show advanced settings... option.



● Open the New Tab page

○ Continue where you left off

○ Open a specific page or set of pages. Set pages

Appearance

☑ Show Home button

New Tab page Change

☑ Always show the bookmarks bar

Search

Set which search engine is used when searching from the omnibox.

Users

You are currently the only Google Chrome user.

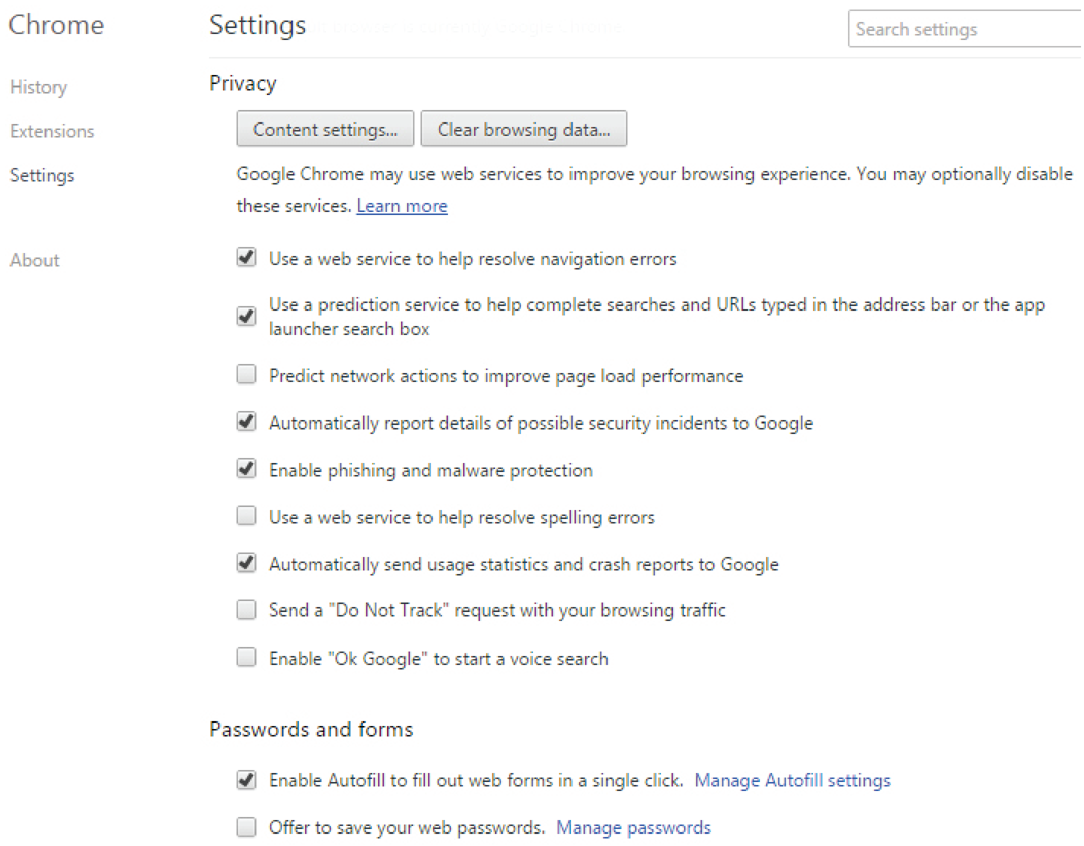
Default browser

The default browser is currently Google Chrome.

Show advanced settings...

Click the link in order to access the advanced settings available.

2. Privacy Settings



Privacy

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

☑ Use a web service to help resolve navigation errors

☑ Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box

□ Predict network actions to improve page load performance

☑ Automatically report details of possible security incidents to Google

☑ Enable phishing and malware protection

□ Use a web service to help resolve spelling errors

☑ Automatically send usage statistics and crash reports to Google

□ Send a "Do Not Track" request with your browsing traffic

□ Enable "Ok Google" to start a voice search

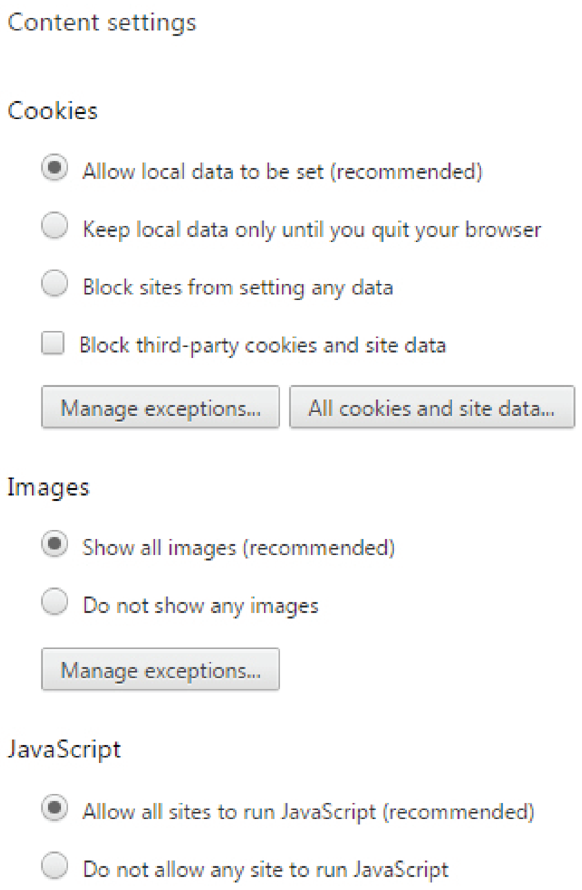
Passwords and forms

☑ Enable Autofill to fill out web forms in a single click. Manage Autofill settings

□ Offer to save your web passwords. Manage passwords

The Clear browsing data… option gives you the possibility to delete your browsing history, so don’t forget to use that option if you are using a computer in a shared environment.

The Content settings… option gives you more possibilities to address and improve your overall browsing security.



Content settings

Cookies

● Allow local data to be set (recommended)

○ Keep local data only until you quit your browser

○ Block sites from setting any data

□ Block third-party cookies and site data

Images

● Show all images (recommended)

○ Do not show any images

JavaScript

● Allow all sites to run JavaScript (recommended)

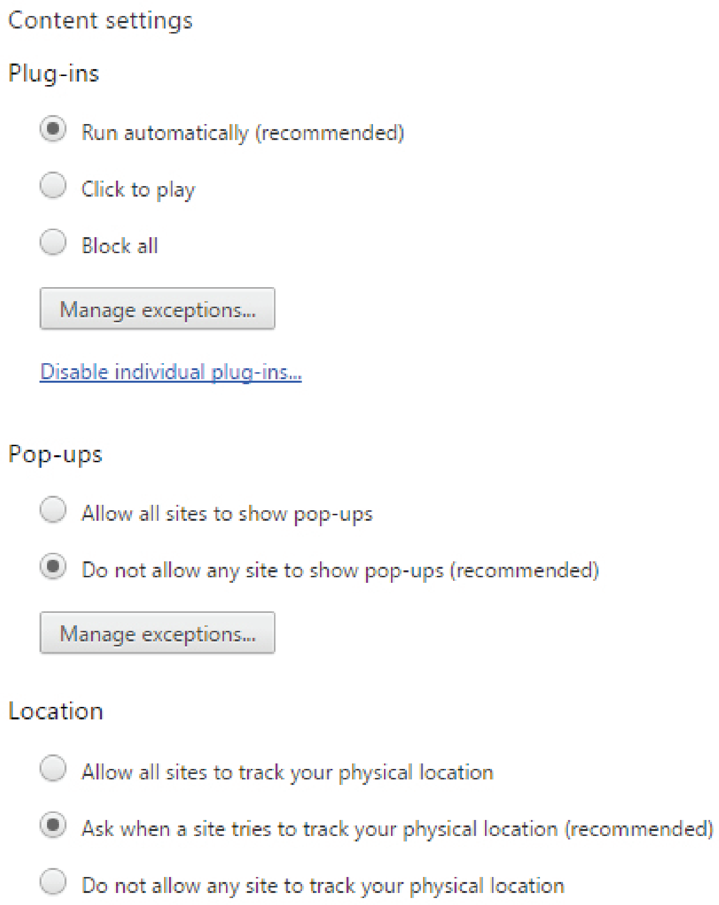
○ Do not allow any site to run JavaScript

To make the necessary changes in the **Content settings** window, you will need to scroll down in order to access the other options.

If you want to **restrict cookies** from being stored on your browser and using the collected information about your browsing habits, use the available options. Another option in that area is to **disable JavaScript**, a vulnerability issue exploited by hackers over the years.

Scrolling down, you find other options:

Lesson 10



Content settings

Plug-ins

● Run automatically (recommended)

○ Click to play

○ Block all

Pop-ups

○ Allow all sites to show pop-ups

● Do not allow any site to show pop-ups (recommended)

Location

○ Allow all sites to track your physical location

● Ask when a site tries to track your physical location (recommended)

○ Do not allow any site to track your physical location

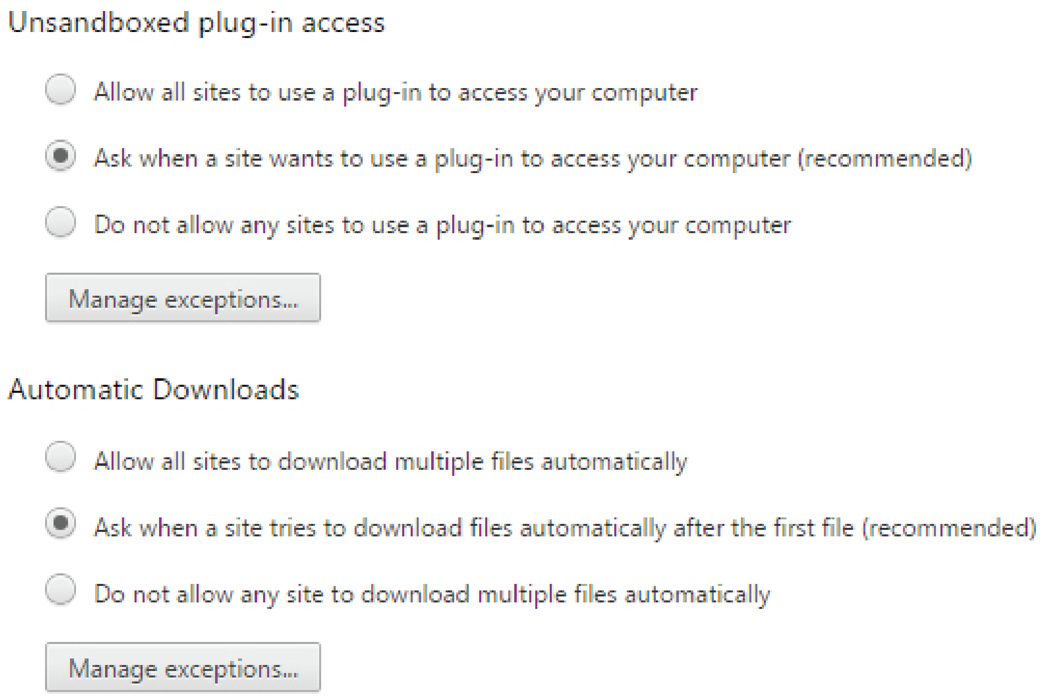
3. **Plug-ins**
   You can **control the behavior of your browser plug-ins** and decide if your browser plug-ins should start automatically or not.

4. **Pop-up Blocker**
   You can **block pop-ups** from disturbing your browsing sessions.

5. **Location Tracking**
   Or, you can stop a website from tracking your physical location

6. Plugin Access Control

If you continue scrolling down to the bottom of the **Content settings** window, you will find the option to **block websites** from using a plug-in to access your computer.



Unsandboxed plug-in access

○ Allow all sites to use a plug-in to access your computer

● Ask when a site wants to use a plug-in to access your computer (recommended)

○ Do not allow any sites to use a plug-in to access your computer

Automatic Downloads

○ Allow all sites to download multiple files automatically

● Ask when a site tries to download files automatically after the first file (recommended)

○ Do not allow any site to download multiple files automatically

7. Automatic Download

There is also available the option to block sites from downloading multiple files automatically on your computer, which is a possible vulnerability that could affect your online security.

5 extensions for a better online session

To improve your browser security you had to make minor adjustments to your web browser, but for a complete protection in the online environment, you need to install some of the best extensions available.

Browser extensions are small software programs that improve and personalize your online experience. With so many extensions (or add-ons) out there, it is difficult to make the right choice. Some of them address your need for privacy, others your need for protection and security while browsing on various websites, from sites where you pay taxes to sites where you simply access your online banking account. Since there is a long list, I will try to present you only some of the best extensions that **block sites from tracking** you, **block ads** and scripts and **keep you safe on unknown** web locations.

Using a browser extension you have a greater control over your browser behavior. You can block ads from some websites and pop-ups that may act like carriers for financial and data stealing malware. At the same time, you have the possibility to block others from breaching your privacy settings. But, you should also be aware that you need to test these extensions and know what they are capable of doing.

Block ads and pop-up windows with AdBlock Plus

AdBlock Plus is an extension for Mozilla Firefox and Google Chrome that can be used mainly for blocking ads and pop-up windows. It has the ability to stop you from accessing web locations controlled by hackers and it can also disable third-party tracking from websites. It is easy to use, without losing time with too difficult to use settings and options.

Don't want to be tracked? Use Disconnect *and* Do Not Track Me

There have been some talks recently in the online environment about finding the best solution for stopping companies in tracking your browsing habits while navigating online.

Disconnect, available for Mozilla Firefox, Google Chrome and Internet Explorer is a very useful extension which manages to:

- block third party tracking cookies
- control the scripts on the site using a simple toolbar menu
- blocks your social media account from tracking your browsing history and private data

Do Not Track Me, available for Mozilla Firefox, Google Chrome and Internet Explorer, comes with a browser toolbar that indicates the tracking cookies, scripts and plug-ins that function on the site and gives you the option to choose which one you want to disable, leaving the others to continue working.

***Stay safe with** HTTPS Everywhere **and** Web of Trust*

HTTPS Everywhere, available for Mozilla Firefox and Google Chrome, is a popular security tool for online browsing. In a few words, what this extension does is to look for secure versions of the websites you access and use them, instead of their lesser safe versions. If you encounter issues with some websites that don't work on **https://**, you simply place that website on a list so that you may access it.

Web of Trust, available for Mozilla Firefox, Google Chrome and Internet Explorer, ranks websites by reputation and helps you establish if the site you want to access has hosted malware or contains tracking cookies which could affect your system security. Though it doesn't block ads from that web location, it helps you by mentioning the rank of the site you want to access and gives you the option to make a conscious decision on your next step.

Lesson 10

In this fight for online protection, keeping your main tool – the **BROWSER** - secure is a vital step. That is why your operating system defense should contain multiple layers of protection, from security products to the web browser, the central tool we use to access our social media accounts, our email addresses and our online banking websites.

Though you may already have a security product right now, just remember you can always return to this guide when necessary and choose the best antivirus solution for your system.

Lesson 11 /19

Are you protected from cyber attacks delivered via Wi-fi? Find out:

Lesson 11

Hi there,

In the previous lesson we talked about increasing online safety by adjusting the browser's security settings, *but do you know how to protect your valuable data on* ***public Wi-Fi networks*** *that are anything but safe?*

Home Wi-Fi Networks (jump to section)
Public Wi-Fi Networks (jump to section)

And how exactly do you increase security on your own ***home Wi-Fi network?***

Before we follow the steps that should be taken to increase protection for a home wireless network, I would like to give you some valuable insights on how to defend your privacy on public wireless networks.

So it is okay if I use public WI-Fi to buy stuff online, check out my online banking account or entering passwords to crucial websites?

The answer is simple: **No**.

That's because public networks can be quite easily breached by hackers and malicious software.

And if you have no choice but using them, you need to employ a few tricks or follow some general guidelines to avoid any possible intrusion or identity theft.

Lesson 11

11 Security Steps to Stay Safe on Public Wi-Fi Networks

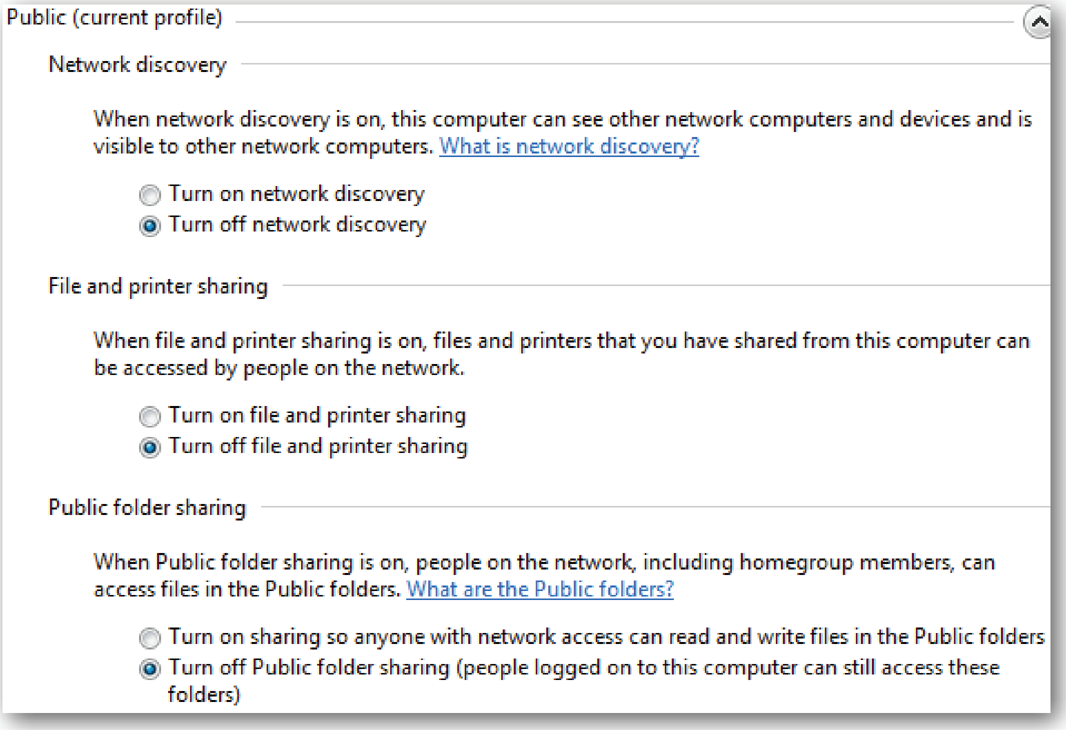
1. Turn off your public network sharing options

If you're using your home or work network you may feel safe enough to allow network resources sharing, like printers or public folders, but on an unsafe public network, this is not recommended. Usually, **the public wireless networks are not subjects to high levels of security and are favorite places for hackers and malicious software.**

To turn off public sharing, follow these steps:

1. Go to your Windows **Control Panel**.
2. Access the **Network and Sharing Center** window.
3. Click **Change Advanced Sharing Settings**.
4. Select the **Public** profile.
5. Turn off **File Sharing, Network Discovery,** and **Public Folder Sharing**, in case they aren't already OFF. Usually, by simply choosing that you are connecting on a Public network, these options are automatically turned off. **(The steps may differ on different Windows operating systems.)**

Lesson 11


Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file and printer sharing
● Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

○ Turn on sharing so anyone with network access can read and write files in the Public folders
● Turn off Public folder sharing (people logged on to this computer can still access these folders)

2. Keep the Firewall Enabled

Make sure your Windows firewall is turned on. If you are using a security product that provides a better firewall, make sure it is still enabled. Sometimes, when you're trying to access an online location and notice a slow-down, you disable it temporarily and forget to enable it back.

To check, access the **Control Panel** window, go to **System and Security** and select **Windows Firewall**.
(The steps may differ on different Windows operating systems.)

3. Use secure websites for sensitive operations

First of all, I don’t recommend running any important operation or financial transaction on a public wireless network. This being said, if you still need to use a public network to check your bank balance, make sure you visit a secure website.

To know you’re using a secure site, look to the left of the web address and find the “Lock” icon. This indicates you are on an encrypted or verified location.
At the same time, check the web address starts with **“https://“**. The **“S”** is from **“secure socket layer”** and you know you are going to a site where communication is encrypted.

If you don’t want checking all the time the web address, use **HTTPS Everywhere**, which is available for Firefox, Chrome, and Opera. This little extension has the role to encrypt your communications with many major websites, making your browsing more secure and safe from online criminals.

Even if you don’t use this extension, many sites like Facebook or Gmail use https automatically. In the end, we’ll say again that sensitive browsing, where important credentials or financial data are used, should not be run on public networks.

4. Use a Virtual Private Network

Public networks are favorite places for cybercriminals to retrieve sensitive data by using wireless sniffers in order to obtain communication details sent over the unsafe network.

To increase your connection security you can use a ***"private browsing"*** session, which means that your browsing history will not be kept locally. But this doesn't mean that the Internet Service Provider or the network administrator will be blocked from ***"listening"*** to your online session.

For a greater degree of security, you can start using a **VPN**, which is a **Virtual Private Network**.

The VPN hides your IP address by encrypting your connection and allowing you to browse online in anonymity. Using this method you protect your online privacy and you keep your valuable information from cyber threats, online scams, identity breaches or phishing attempts.

To keep your online session private on public wireless networks, I recommend a popular VPN solution like **CyberGhost**.

5. Turn the Wi-Fi connection OFF

Are you done using the Wi-Fi network? Then don't forget to turn it off.

There is no reason to stay connected more than you need. The more you stay connected, the more chances are for your system to be noticed by cybercriminals or malicious software. At the same time, this helps your laptop save the battery life.

6. Update and patch everything

Keep your Windows operating system up-to-date

Always keep your system up-to-date with the latest security updates and patches available.

To take the security updates automatically, follow these steps:

1. Go to your Windows **Control Panel** window.
2. Select **Windows Update** and click **Change settings**.
3. Make sure **Install updates automatically** is selected.

It is important to have the latest security updates for your Windows operating system, because they contain stability fixes and patches that keep your system safe from cybercriminal attempts that try to benefit from any security hole.

Update your software with the latest patches

I know that online criminals try to benefit from security holes in popular software we use on our computers, like Java, Adobe Flash or popular web browsers like Chrome, Mozilla or Internet Explorer.

For this reason, I would recommend you have the latest updates or security patches for the software you are using. Or if you don't want to bother checking and keeping the vulnerable applications up-to-date every day, I recommend using a free dedicated **solution** to do the job.

7. **Don't connect to a public network without a reliable antivirus**

   It is important to have a good antivirus product from a big security company, which should include real-time scanning, firewall and automatic update capabilities. Go back to **lesson 5** If you need advice on how to pick the right AV for your system (and budget).

8. **Don't browse without a good anti-spyware solution**

First, what do you mean by spyware?

Without going into too much information, Here's how your system would behave if it were infected with spyware:

- pop-up windows are everywhere
- error messages appear without notice and they don't seem to go easily
- web browser search engine has been replaced with something fishy
- web browser home page is not the one you set
- unknown toolbars appear in your browser
- slow down affects every step you take

How do I become a spyware-fighting hero?

Spyware can affect us on any type of network, but on an open public network the online dangers could affect our computers even more.

To keep your system protected from spyware, I need to point out the importance of using anti-spyware solutions from well established companies in the online sphere, like **Spybot Search and Destroy, Lavasoft's Ad-Aware, Malwarebytes** and others.

And finally, I just have to say it again. Even if you install

20 security solutions to keep you safe online, unless you adopt some good security practices you won't be safe online:

- stay away from clicking fishing links or random pop-up windows
- don't reply to strange questions in your web browser or your email inbox
- don't just go online downloading any application you see

9. Don't run financial transactions without special protection

I have to say it again:

I strongly advise against running financial transactions or inserting sensitive or valuable information when using a public unsafe network!

Nevertheless, if you Really, really, REAAAAAAALLY need to access your bank account or pay online, I recommend a special security **solution** that can stop malicious software from retrieving sensitive data and block cybercriminal actions before they affect your system.

Next-gen anti-hacking tools (the stars of **lesson 6**) are an extra security layer that aredesigned to complete your online safety.

10. Secure your browser before you go online

We go online by using our web browsers and for this reason, we need to secure these tools correctly before we access any website.

And let's not forget that browsers are applications which, without the proper security updates, may become access doors for online criminals that attempt to steal data by using unpatched security holes.

Therefore, to increase the online security, especially when using a public wireless network, follow these guidelines:

- Make sure you have the **latest browser version** and you have installed the latest security patches.
- Access and modify your **browser's security settings**. Go back to **lesson 11** for step-by-step instructions (and actually change your settings, if you haven't yet).
- Use the **private browsing session** before you access a website. This option will not keep your browsing history recorded locally. After selecting the private browsing session, go to your search engine and look for **free proxy** or something similar, access the proxy and insert the website address you want to reach. There are many free

proxy sites online, so it's quite easy to find one.

- For an increased protection, download online a popular and reliable VPN software, like **CyberGhost**, and make sure data you send and receive is encrypted and cannot be accessed by prying eyes.

11. Use two-factor authentication everywhere

This option is actually an extra security step that can protect your popular online account. It may be your Facebook, Twitter or Gmail account. Or it may be any other online account that provides the two-factor authentication.

This extra security step increases your online protection by making sure that besides your credentials, which may be retrieved by hackers, **you are required to enter an additional one-time code, which is sent to your mobile phone.**

It is always useful to consult an extended **list** of programs and web apps, before selecting one for your system.

The steps above can be followed on public Wi-Fi networks to increase your data protection. At the same time, don't forget we are talking about some of the less protected areas of the Internet and you should avoid running important sensitive actions in this spaces.

Home Wireless Network Security

Though somehow less exposed to hackers and other dangers that exist on public wireless networks, **our own home Wi-Fi networks can also become targets to cyber-criminal attacks.**

Present households shelter a number of mobile devices that are linked to the Internet and we are not talking just about laptops and mobile phones, but TVs and other **devices** that we include in the **Internet of Things** area.

And this **connectivity between our devices poses security risks for our private data and sensitive financial information.**

Though relatively easy to use and access, **Wi-Fi networks are not always SAFE networks**. For this reason, we need to learn how to protect our wireless home networks from malicious intrusions.

10 Steps to Maximize your Home Wireless Network Security

1. Change the name of your home wireless network

As soon as your home wireless network has been set in place, you need to change the **SSID** (Service Set Identifier). This is the **name of your home network**, the name other mobile devices will see when trying to connect to the Internet by using the wireless network from your home.

The reason you need to change its name is quite easy to guess. Modifying the name **increases the difficulty for a hacker** to gain access to your network.

Usually, router manufacturers assign the name of the company that produced the router and it could be something like “**Linksys**“, “**Cisco**” or “**Belkin**“.
In case the SSID is not modified, a hacker has a better chance of breaking into a network, **simply by knowing the manufacturer of the router**. Use this guide to make the necessary changes.

And one more thing related to this step: **Do not use your name or your family name in order to avoid being identified as the owner of the network.** This is another detail that could give an advantage for a potential hacker or for an online criminal that might attempt an identity theft operation.

2. Choose a strong and unique password for your wireless network

Your wireless router **comes pre-set with a default password**. The problem is that **this default password is easy to guess by hackers**, especially is they know the manufacturer's name for the router. See step 1 above.
When setting a good password for your wireless network, **make sure it is at least 20 characters long and includes numbers, letters and various symbols.**

This setting will prevent other people from accessing your network. Though usually, it is nothing more serious than some neighbor **"stealing"** from your network bandwidth speed, you may have to deal with other more challenging situations, like **online criminals that can access** your network to **"listen" to your traffic data and retrieve sensitive information.**

Increase your security by enabling network encryption

There are a few popular encryption options for wireless networks, like **WEP,WPA** and **WPA2**. The latter form of encryption – **WPA2** – is preferred for its improved security and especially if you have a home network.

The option to **encrypt traffic is useful if you need to make your communication signals unusable** for any unauthorized third party software.

At this moment all wireless devices out there support this technology and it is common knowledge to use **WPA2**, which has a greater degree of security.

4. Disable the wireless network when you're not at home

This option is useful especially when leaving home for extended periods of time, for a vacation or for a few days.

This security measure, besides helping you to reduce power consumption, **it will surely stop any hackers that could "listen" to your network's traffic or might try to access it for malicious purposes.**

5. Where in hour home did you set up your router?

It could be a good idea to **place the wireless router as close as possible to the middle of your house.** And it's not just for every place or room in the house to have same access to the Internet, but because **you don't want to have your wireless signal range reach too much outside your house**, where it can be easily received by hackers.

For this reason, don't place it too close to a window, from where the signal can be easily accessed from outside, even at some distance, and you may also follow our fourth rule to **disable the router when leaving your home.**

6. Choose a strong password for your network administrator

To set up your wireless router, usually you need to access an online platform or web page, where you can make modifications to your network settings.

As everybody knows, it is something normal to find a router **with default credentials such as "admin" and "password"**. And these default login credentials are not so difficult to break by a hacker.

Most changes we do on an online platform are things like setting a strong password for the wireless network or changing the network's name, both changes being made to ensure a greater level of protection from online criminals' malicious actions.

But if an IT criminal is able to access the administrator platform and gain access to your network's setup and configuration settings, this will ruin your day for sure.

7. Disable Remote Access

Normally, you can access your router's interface from a device connected to your network, but some routers allow access even from remote systems. **To stop online hackers access to your router's private settings, it is safe to disable this option in your router's settings.**

To make this change, access the web interface and search for **"Remote access"** or **"Remote Administration"**.

8. Keep your router's software up-to-date

Consider your router's software like any other software you have on your operating system. It may be your antivirus program or any other application running on the system. **The router's firmware, like any other software, contains flaws which can become major vulnerabilities, unless they are quickly fixed by firmware releases from the manufacturer.**

The problem is that most routers don't have the option to install the latest security updates and from time to time you need to check the official website for security fixes.

We must not forget that some of the worst security breaches came from security holes in unpatched programs and operating systems.

9. Make sure you have a good firewall

Some routers have their own **firewalls that can help block**

hackers from accessing your computer.

In case your router doesn't have such a firewall, make sure you install a good firewall solution on your system to watch for malicious access attempts to your wireless network.

These days, most people use the firewall solution provided by their operating systems, which is a good option. In case you are using a security software that contains a firewall, it is a good option to turn it on.

10. Protect the devices that connect most frequently to your wireless network

Don't leave any door open for online criminals!

Though you may have secured your router and your wireless network, you need to **make sure you are not leaving any security breach that can be exploited by IT criminals.** Therefore, follow some general and common sense guidelines to stay away from online dangers, like having the **latest software available** installed on the system and the **latest security patches downloaded** to ensure no security hole or breach is left open to online predators.

Even more, check what devices connect mostly to your home network and make sure they have **security soft-**

ware installed against the viruses and spyware.
And finally, **use a specialized security software to protect your devices from financial and data stealing malware,** cybercriminals and malicious hacker servers.

Wi-Fi networks symbolize the power of Internet, its freedom to spread knowledge and information everywhere and at almost no cost.

At the same time, these networks are not the most secure places on Internet and cybercriminal minds are lurking everywhere.

To continue using a public or a home network, you need to make sure you followed some of the steps above.

I tried to be thorough in this lesson and cover both public and home Wi-Fi networks.

This way, you have all the security steps to stay safe on wireless networks and you can always return to this guide when necessary to increase your online protection.

Lesson 12 /19

Keep cyber criminals out of your inbox for good. Here’s how

Just like me, you probably have various social media accounts, banking accounts and we often subscribe to many sites and online services.

But, if you can unsubscribe from a site, close or change your social media platform and even change the bank, you definitely keep your email address for a long time.

At the same time, for the same reasons I mentioned above, no one can actually stay online without an **email Account**.

And it's not just about confirming your websites subscriptions, ***but where else could you receive any private data from an online location, if not directly to your personal email address?***

And by private data I mean: **financial operations, passwords, professional details and sensitive information.**

For an **IT criminal**, getting access to your email account is the first step in operating an **online identity theft**. Therefore, this vital component cannot be ignored and treated easily.

Before I mention all the necessary steps you can take to improve your online email account security, **you need to take a quick look at the most popular web-based email services and the security options you can take** for each one of them.

Though there are many other online email services, I will include in this security analysis only the 4 most popular web-based email providers at this moment: **Yahoo!, Gmail, Aol** and **Outlook.**

The final part of our security analysis consists in presenting the **general guidelines you need to follow to keep your online email account safe.**

The Complete Guide to Email Security

Yahoo (jump to section)

Gmail (jump to section)

Aol (jump to section)

Outlook (jump to section)

Protect Your Yahoo! Mail Account

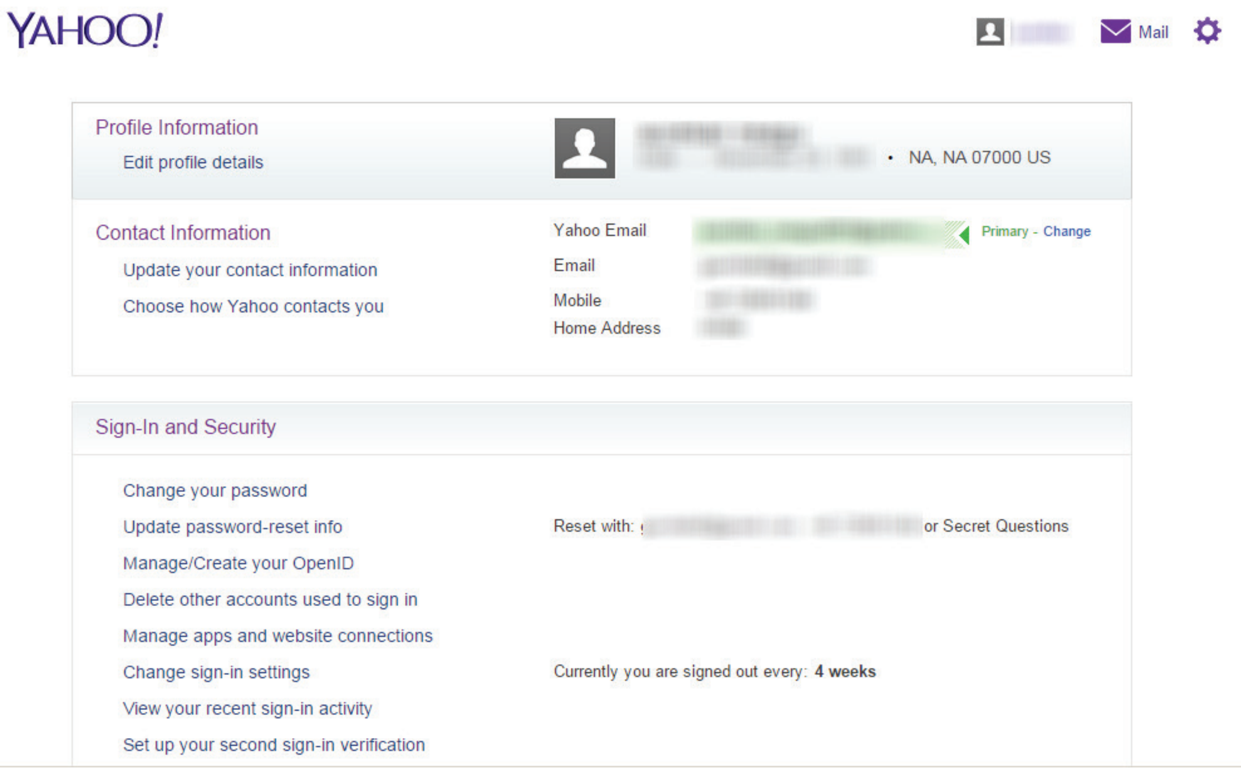
Yahoo! mail service is probably the most popular email account in the world at this moment. How many of us didn't create an email address with Yahoo! *more than 10 years ago?* So, our relationship with this email provider goes a long way and we cannot ignore it.

To make the necessary changes in your email account,

Lesson 12

you need to access your Yahoo! mail profile settings:

To make the necessary changes in your email account, you need to access your Yahoo! mail profile settings:



Profile Information
Edit profile details
[redacted] · NA, NA 07000 US

Contact Information
Update your contact information
Choose how Yahoo contacts you

Yahoo Email [redacted] Primary - Change
Email [redacted]
Mobile [redacted]
Home Address [redacted]

Sign-In and Security

Change your password
Update password-reset info — Reset with: [redacted] or Secret Questions
Manage/Create your OpenID
Delete other accounts used to sign in
Manage apps and website connections
Change sign-in settings — Currently you are signed out every: **4 weeks**
View your recent sign-in activity
Set up your second sign-in verification

1. Update your contact information

It is important to add an **alternative email address and a mobile phone number** so that you may be contacted in case of trouble. If you have problems in accessing your online email account, you can have a recovery link sent to the alternative email address or an SMS message delivered to your mobile phone.

2. Set up your second sign-in verification

This is probably the most important security setting you can set in your Yahoo! account. This second step verification adds an **extra level of protection** for your email address. To activate this security step, you need to add your **phone number** to the Yahoo! account. At the same time, you have the possibility to set 2 additional security questions for an easier access to your online account. Setting these security questions and choosing them for the second sign-in verification allows you a faster and easier access.

3. View your recent sign-in activity

Don't forget to verify your account login history and make sure only you connected to your email address account.

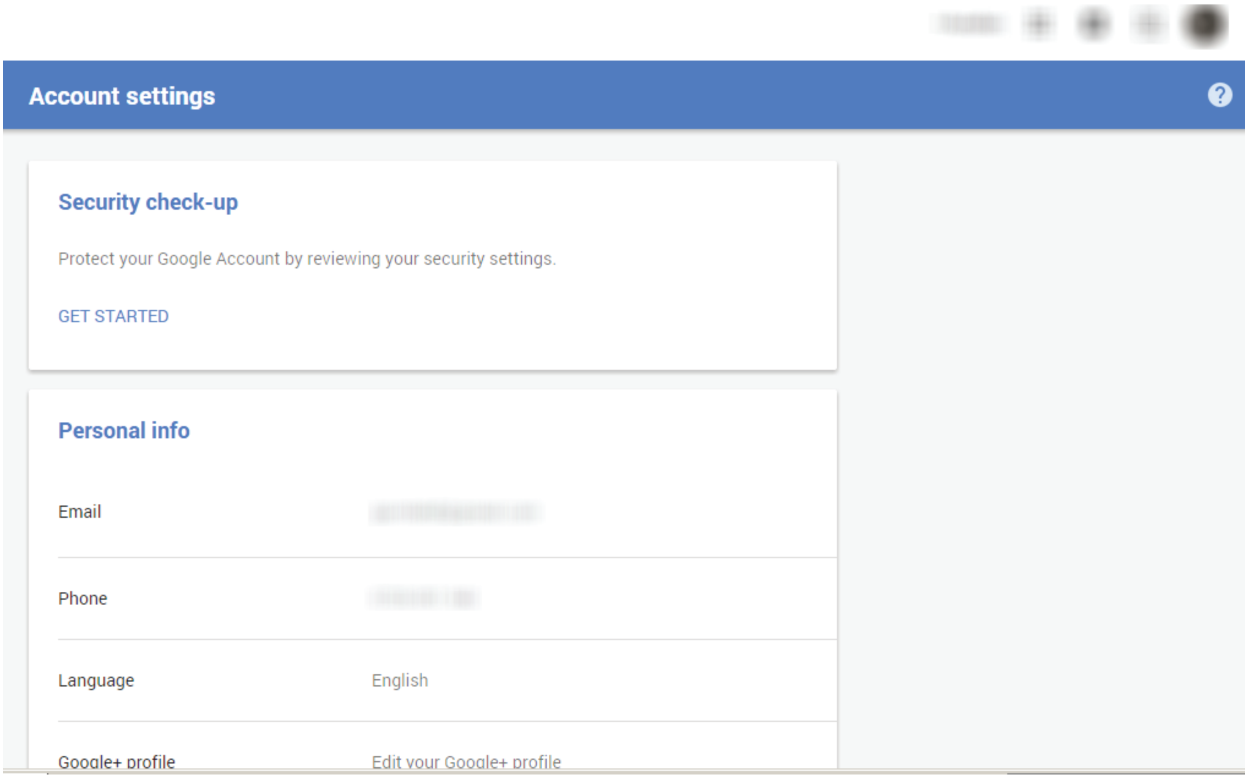
4. Delete other accounts used to sign in

Did you connect to your Yahoo! mail from a different account? This place allows you to remove that connection and all information associated to your account.

Protect Your Gmail Account

Gmail service has become in the recent years – together with Google Chrome – one of the most popular email services and it's being used not only for personal purposes, but also increasingly for professional correspondence.

To make the necessary changes in your Gmail account, you need to access your Gmail settings:



Instead of sending you through all the available steps from that location, I recommend using the **Security check-up** option above and review your Gmail security settings.

Therefore, click **Get Started** and follow these steps:

1. **Check your recovery information**

   The most important security settings available in that location are to **set a recovery phone and an alternative email address**, where you can be contacted in case an unusual activity takes place on your account. In the same location, you can set a **security question**.

   Make the necessary changes and click **Done** to continue.

2. **Check your recent activity**

   Review the connections list to spot any unfamiliar activity. Click **Looks good** to continue.

3. **Check your account permissions**

   Verify the list of apps, websites and devices that are connected to your account. Choose to remove those you don't use anymore and click **Done** to continue.

4. **Check your app passwords**

   Have you generated a password for an app that you don't use anymore? Click **Revoke** or select **Done** to continue.

5. **Check your 2-step verification settings**

   In this location you can make sure you have the verification messages sent to the right **phone number** and you are also able to set up a **backup phone**, in case you lose access to your own phone. For more settings, follow the corresponding link. Click **Done** to finish the security check-up and go back to your account settings.

Protect Your Outlook Account

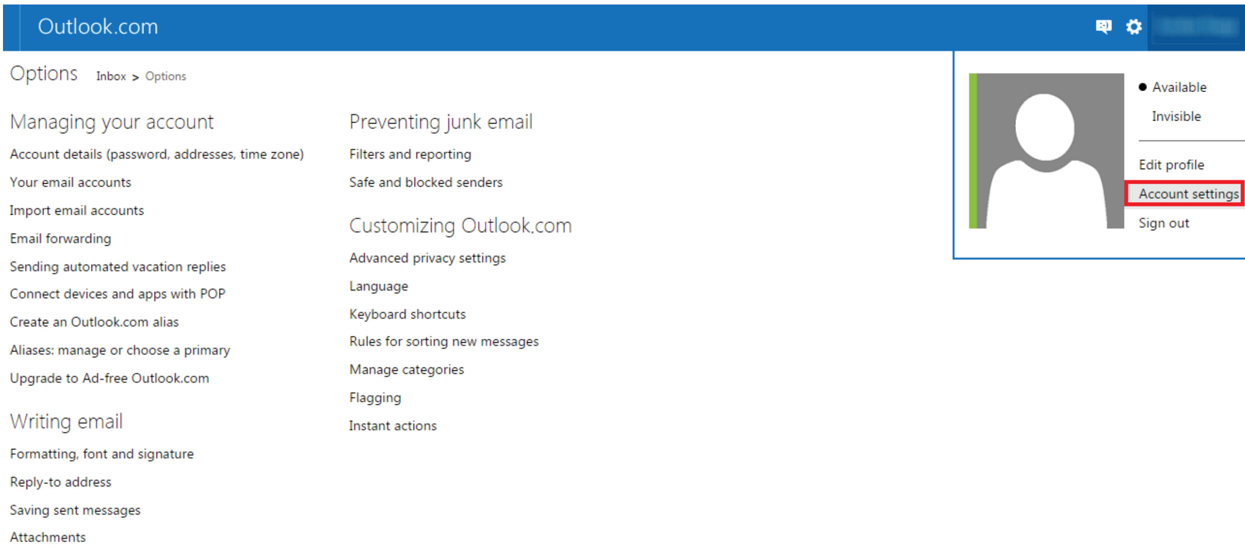
Outlook.com appeared in 2012 and it has replaced the old Hotmail web-based email service provided by Microsoft for more than 10 years.

To make the necessary changes in your Outlook account, you need to access your Outlook advanced settings.

Follow these steps:

1. **Access your profile settings.**

Lesson 12


Outlook.com [redacted]

Options Inbox > Options

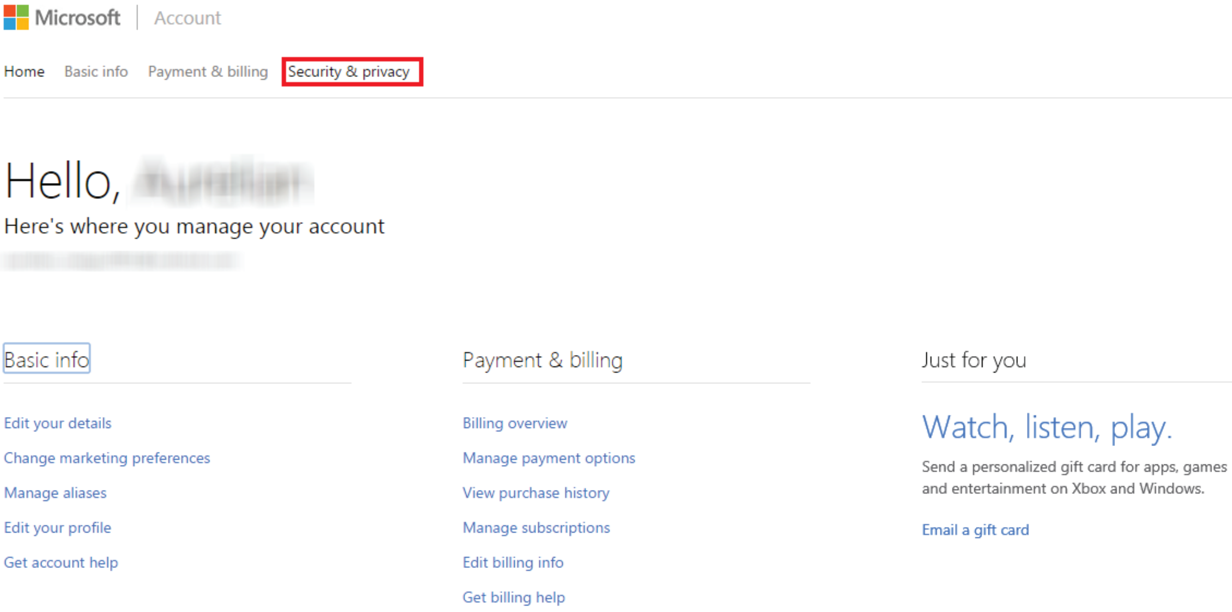
Managing your account
- Account details (password, addresses, time zone)
- Your email accounts
- Import email accounts
- Email forwarding
- Sending automated vacation replies
- Connect devices and apps with POP
- Create an Outlook.com alias
- Aliases: manage or choose a primary
- Upgrade to Ad-free Outlook.com

Writing email
- Formatting, font and signature
- Reply-to address
- Saving sent messages
- Attachments

Preventing junk email
- Filters and reporting
- Safe and blocked senders

Customizing Outlook.com
- Advanced privacy settings
- Language
- Keyboard shortcuts
- Rules for sorting new messages
- Manage categories
- Flagging
- Instant actions

2. Click Security & privacy.


Microsoft | Account

Home Basic info Payment & billing Security & privacy

Hello, [redacted]

Here's where you manage your account

[redacted]

Basic info
- Edit your details
- Change marketing preferences
- Manage aliases
- Edit your profile
- Get account help

Payment & billing
- Billing overview
- Manage payment options
- View purchase history
- Manage subscriptions
- Edit billing info
- Get billing help

Just for you

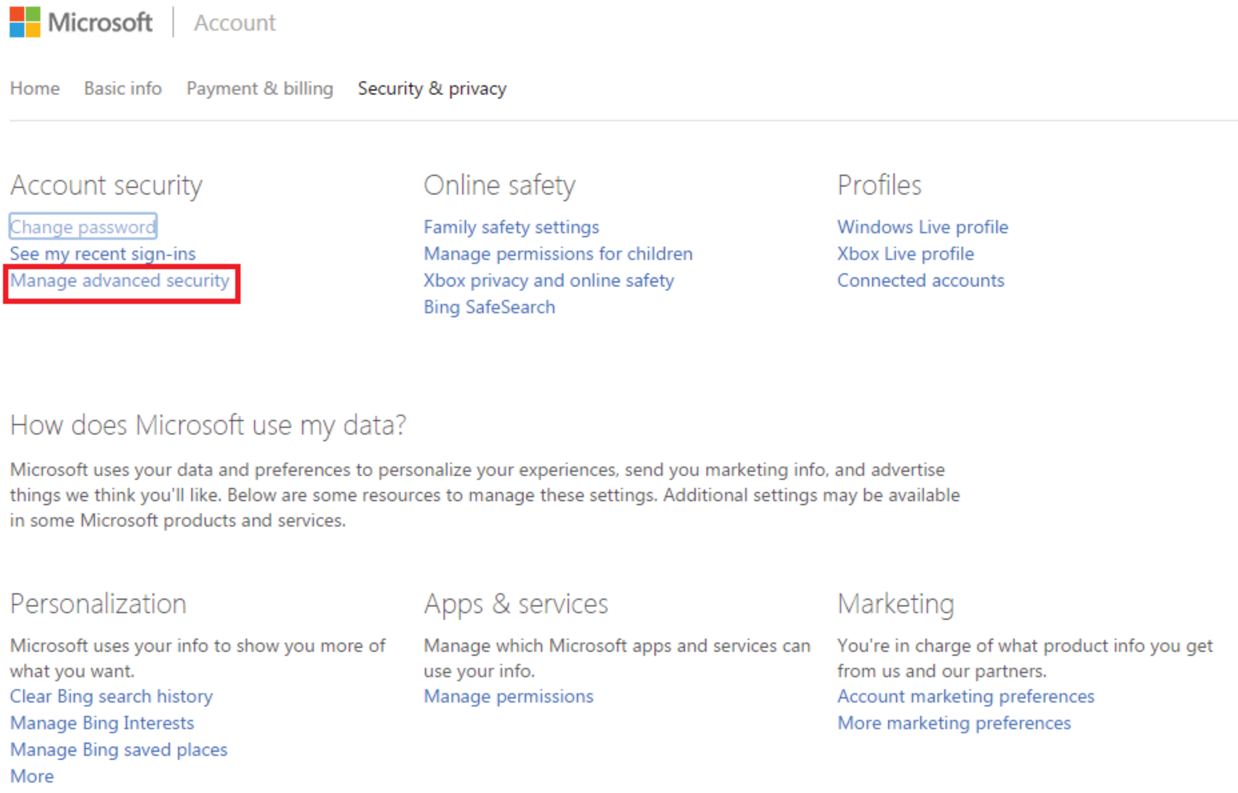
Watch, listen, play.

Send a personalized gift card for apps, games and entertainment on Xbox and Windows.

Email a gift card

3. Choose Manage advanced security in the new window.

Lesson 12



Microsoft | Account

Home Basic info Payment & billing Security & privacy

Account security
Change password
See my recent sign-ins
Manage advanced security

Online safety
Family safety settings
Manage permissions for children
Xbox privacy and online safety
Bing SafeSearch

Profiles
Windows Live profile
Xbox Live profile
Connected accounts

How does Microsoft use my data?

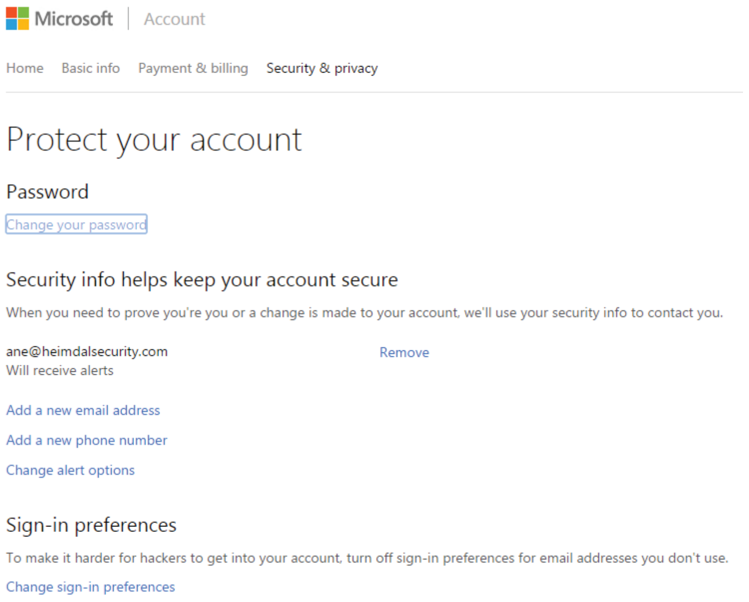
Microsoft uses your data and preferences to personalize your experiences, send you marketing info, and advertise things we think you'll like. Below are some resources to manage these settings. Additional settings may be available in some Microsoft products and services.

Personalization
Microsoft uses your info to show you more of what you want.
Clear Bing search history
Manage Bing Interests
Manage Bing saved places
More

Apps & services
Manage which Microsoft apps and services can use your info.
Manage permissions

Marketing
You're in charge of what product info you get from us and our partners.
Account marketing preferences
More marketing preferences

In this location you can make the necessary changes for your Outlook account.



Microsoft | Account

Home Basic info Payment & billing Security & privacy

Protect your account

Password
Change your password

Security info helps keep your account secure
When you need to prove you're you or a change is made to your account, we'll use your security info to contact you.

ane@heimdalsecurity.com Remove
Will receive alerts

Add a new email address
Add a new phone number
Change alert options

Sign-in preferences
To make it harder for hackers to get into your account, turn off sign-in preferences for email addresses you don't use.
Change sign-in preferences

4. Update your contact information

The most important security change you can make to your account is to **add an alternative email address and a phone number** where you can be contacted.

5. Set up the 2-step verification

Add an extra layer of protection to your -mail account. Click the corresponding option to set-up this security option and decide if you want to connect to your account using a **security code** sent to your phone number, a **smartphone app** or **recovery codes** written down in order to be used later on.

If you go **back**, you have the same options available:

- **Identify verification apps** – to use an app from your smartphone.
- **Recovery code** – to print the recovery codes and keep them in a safe location.
- **Trusted devices** – remove those devices you don't use anymore to connect to your email account.

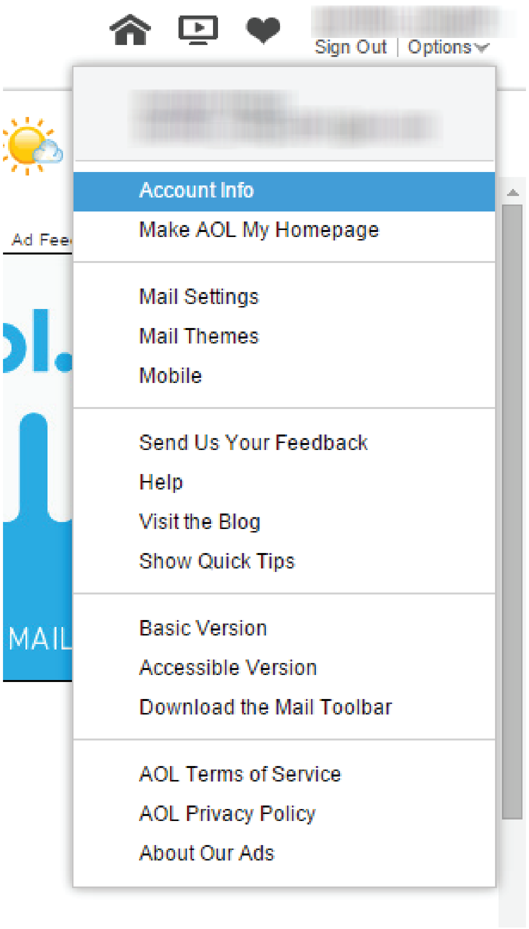
Lesson 12

Protect Your AOL Mail Account

AOL mail service is at this moment among the most popular web-based mail services in the world, especially in the United States.
To make the necessary changes in your AOL account, you need to access your general account information.

Follow these steps:

1. Access your **Account Info** from the top right corner.



Sign Out | Options

Account Info
Make AOL My Homepage

Mail Settings
Mail Themes
Mobile

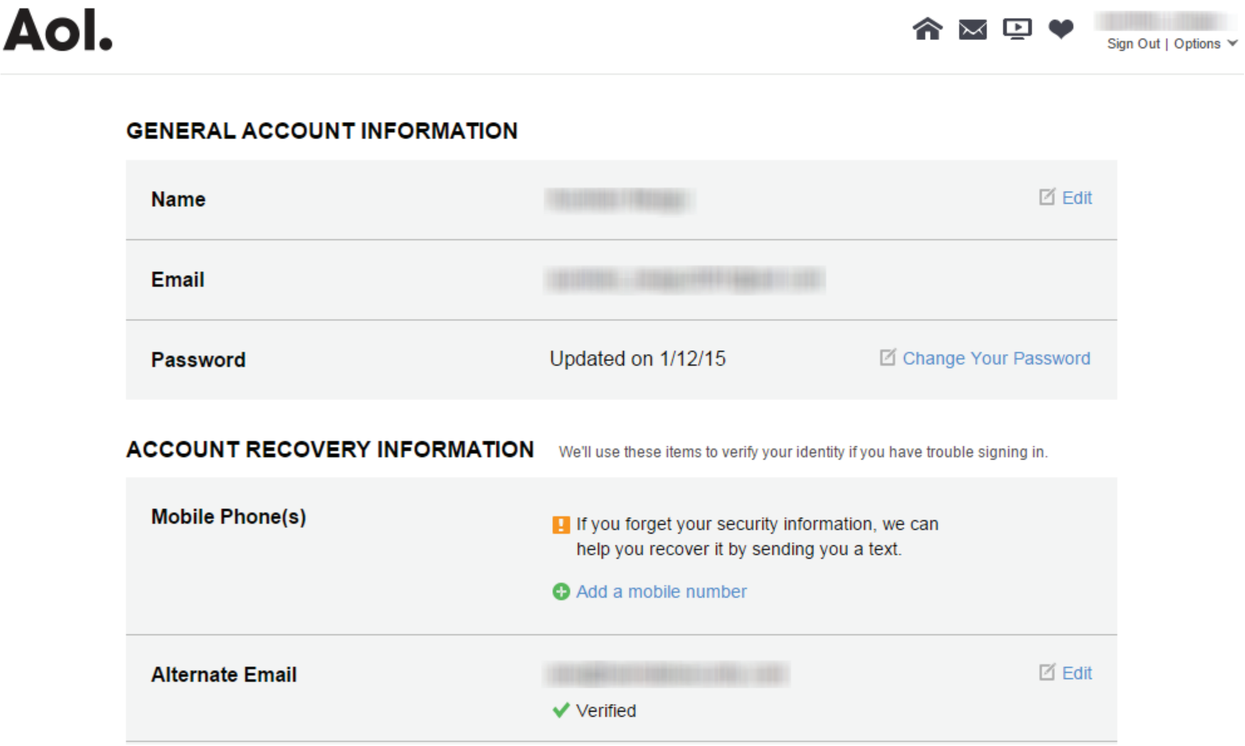
Send Us Your Feedback
Help
Visit the Blog
Show Quick Tips

Basic Version
Accessible Version
Download the Mail Toolbar

AOL Terms of Service
AOL Privacy Policy
About Our Ads

Lesson 12

2. You may need to insert the answer for the secret question you set before getting access to the **General account information.**



GENERAL ACCOUNT INFORMATION

Name		Edit
Email		
Password	Updated on 1/12/15	Change Your Password

ACCOUNT RECOVERY INFORMATION We'll use these items to verify your identity if you have trouble signing in.

Mobile Phone(s)	! If you forget your security information, we can help you recover it by sending you a text. Add a mobile number	
Alternate Email	✓ Verified	Edit

In this window, under **Account Recovery Information**, you have the option to add **an alternative email address and a phone number** where you can be contacted.

12 Guidelines to Complete your Email Security

As you have seen above, the most important security option you can take in our email account settings is **the option to add a second step log-in verification.**

This extra level of protection for your email account means that you'll need to provide an additional security code that you receive to your phone number by SMS. Though I did not find this security option in AOL mail service, I found the options of setting another back-up email address and a phone number where you can be reached in case of trouble.

BUT, email protection is not everything.

To stay safe online, no matter where you are or what you do, you need to think and adopt a strategic vision and imagine a complete security policy. Browsing online, networking on social media platforms, running financial operations or opening an email, **it's all about staying safe.**

To complete your email security, you need to **adopt a strategic vision** and follow these steps **no matter what web-based email service** you are using:

1. **Set a strong password for your account.**

   Make sure you include capital letters, numbers and symbols so that it may be difficult to be compromised. **Don't use the same password** for more online accounts or email services. In case one online account is breached and the particular password for that account is used in other online locations too, you risk having the other accounts accessed by the same hackers.

Remember you can always go back to **lesson 4** on password management when you need to.

2. **Create and use more than one email address**

   To limit the potential information breach, **I recommend using 2 separate email addresses** in order to keep personal data away from professional information.

   This way, you can limit a potential loss in case one of your email addresses is accessed by hackers.

   At the same time, you can add one email address in the other email account's security options and make sure you can be contacted at any moment.

   Make sure you don't use the same password for both email addresses!

3. **Be careful when setting up a security question**

   To set a security question in your email account is a good privacy step and you should not ignore it, if you have this option. But, pay attention and set a question that only you can answer, not a piece of information that anyone can find by simply following your Facebook profile. So, **no**

dog or cat name or anything that you have already shared with the world.

4. **Don't jump connecting to any free public Wi-Fi network**

   I know how happy one can be when discovering by chance a free wireless network in a public space. ***But is your private data safe from a potential IT criminal nearby that can't wait to intercept your communication?***

   Are you really prepared to face an advanced criminal mind, who does this for a living? **No, you're not.**

   But since we know **you won't resist the temptation to go into the wild**, just don't do these 2 things: **don't connect to your email address account and don't run any financial transaction!**

   Resume your online traffic to simple browsing and don't insert any sensitive information.

   Remember the last lesson, the one on **Wi-fi security**? I hope you acted on it. If not, you can still go back to it and do it. ASAP!

5. **Delete all your traffic history when connecting to a public computer**

There are situations when you need to connect to your email address from a public computer in a new location and you're not sure about its security settings. This happens to all of us and it's rather normal. But don't forget to follow a few easy-to-follow steps to stay secure before you leave the public location.

As soon as you finish your online session, make sure you take these steps:

- log out of your email account.
- delete any browsing history, together with any temporary files, cookies are passwords that you may have inserted in the browser.
- close the browser.

To make sure there won't be anything recorded during the browsing period, you better use an **incognito mode** or a **private browsing session**.

6. Choose to use the 2-step authentication option in your email account

I know. I have already mentioned this one, but it is so important that I need to emphasize it again. Choosing to use **this security step demands from you to add a second security code sent by SMS to your phone number.** Use this method to make sure your online accounts are accessed only by you.

Though the first three email services above provide this security option (and **I recommend you to use it**), there are other email providers that have not included the 2-step authentication yet. Since I am a big fan of this security option, I recommend you using an email service that provides this important security step.

7. Avoid phishing email scams

Most successful online scams have always started with an initial email message sent to a potential victim. Though an online scam can occur on social media networks or when you shop online, most infamous scams have always seemed to appear by email.

Since I cannot mention here most popular online scams, I have to mention the **dangerous phishing emails, which are supposed to convince the victim click an email link or download/run an email attachment.** As soon as this action takes place, a malicious software is installed on the system or the victim is sent to a login page from a fake website in order to operate identity theft or retrieve the banking credentials.

This is one of the most popular **hacking techniques to steal financial information** and usually there is no other way to stay safe from this malicious attempt, but prevent the initial infection phase.

8. **Use a good antivirus product that offers real-time protection**

   A reliable antivirus software is important for your overall system security. One that contains **a real-time scanning option** is even better. Though most web-based email services offer antivirus scanning, if you receive an archived password-protected file from someone, a potential infection won't be detected and removed.

   For this reason, you need to have on the system your own security **software with a real-time scanning module**, so that any downloaded and decrypted file could be scanned as soon as possible.

9. **Keep your software updated**

   Most software vulnerabilities occur when we miss to install the latest security updates and patches. It may be your operating system or your vulnerable applications and software, it is important to keep them all up to date.

   Are you using popular applications like Adobe Acrobat Reader, Java, Adobe Flash, Adobe Shockwave or web browsers like Chrome, Mozilla Firefox or Internet Explor-

er? Then you better make sure you have the available patches installed.
In case such an unfortunate event affects your system, try to limit the potential losses by using different credentials for your email address and your online accounts.

10. Keep your private data safe online

- Don't use private information on social media networks.
- Don't use family names as passwords.
- Don't reply to suspicious emails with sensitive information.
- Check your email account activity and your social media profile connections.

11. Use a specialized security software against spyware

One of the most popular ways of spreading spyware is by email **spam campaigns**. I know that you are always careful with your email address and the emails you receive in your inbox. But **it takes only one wrong click on a malicious link or an email attachment and spyware is installed on your system.**

Since **it is better to prevent and take action sooner than later**, I recommend using a reliable anti-spyware product. You can find online a few good anti-spyware products like Spybot Search and Destroy, Lavasoft's Ad-Aware, Malwarebytes, etc.

And again, if you receive a strange suspicious email, follow these simple guidelines:

- don't click suspicious links in emails
- don't reply an email if you're not sure about the sender
- don't download or click email attachments that seem unsafe for your system

12. Access your web-based email service from a secure browser

Most of us use an email address from a browser, so it is an important part of our online security strategy. Not to forget that any vulnerability from our browser may become very valuable for a hacker.

To access your emails in complete security from a secure browser, follow these steps:

- choose **the latest version for your browser and make sure the latest security patches** are installed. Don't leave any door open for a cybercriminal.
- access and **increase the security and privacy levels** in your browser.
- are you accessing your online email address from an unsafe public computer or from a web browser you don't

trust? In this case, choose to go for a private browsing session and **avoid having your browsing history, credentials and other details stored** by the web browser.

Lesson 10 will teach you all about browser security.

Thanks for sticking with me until the end!
I hope this guide will help you increase online security for your email account.

The possibility to hack an email address is a tempting action for any criminal mind, since in this location you often keep banking and financial information, usernames and passwords for our online accounts.

If you think about the Internet as a big bad world where you can just walk around and interact with other people or with public and private entities, then **the email address account can be considered as your HOME.**

And what else is more important to protect?

Lesson 13 /19

Share. Tweet. Protect. Repeat. Social media, the safe way

Lesson 13

Social media is part of our lives. And many times, when you think about social media, you tend to think of **Facebook, Twitter** and **LinkedIn.**
Facebook, for example, spread so much that even our parents, neighbors and distant relatives (even from remote areas of the country) now have a **Facebook** account.

Since these social platforms are so popular and the distinction between public and private is blurred, these online services attract dangerous elements that are interested in retrieving our sensitive information. And in this point you may become a victim to identity theft and malicious actions from online criminals.

So, how do I balance using social media and keeping confidential information confidential?

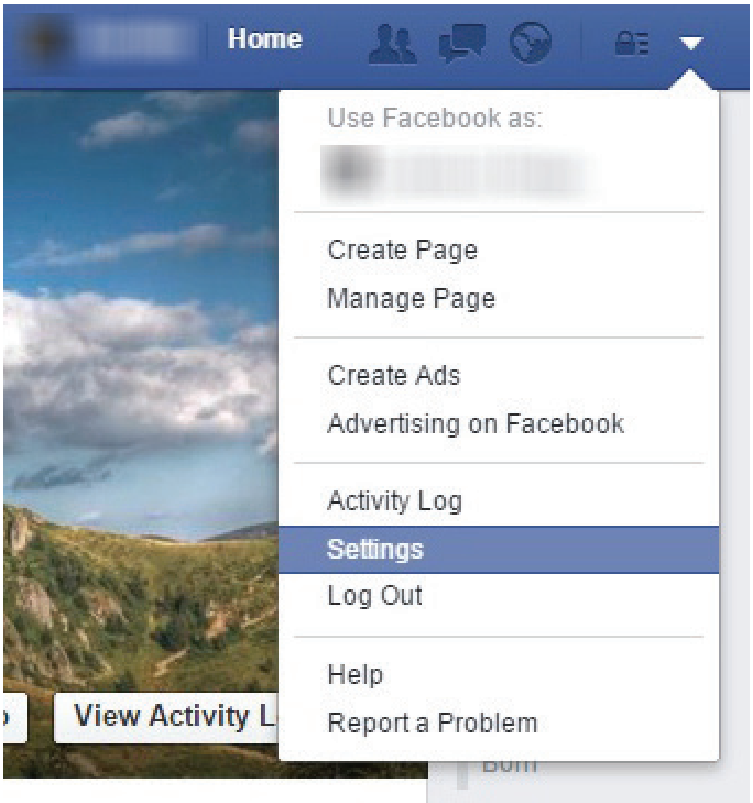
Lesson 13

Protect Your Facebook Account

Since Facebook is probably the biggest and most popular online network right now, I will try to go deeper into this platform's privacy and security settings and then present shortly 10 additional steps you can follow to stay safe online.

Access your Facebook Settings

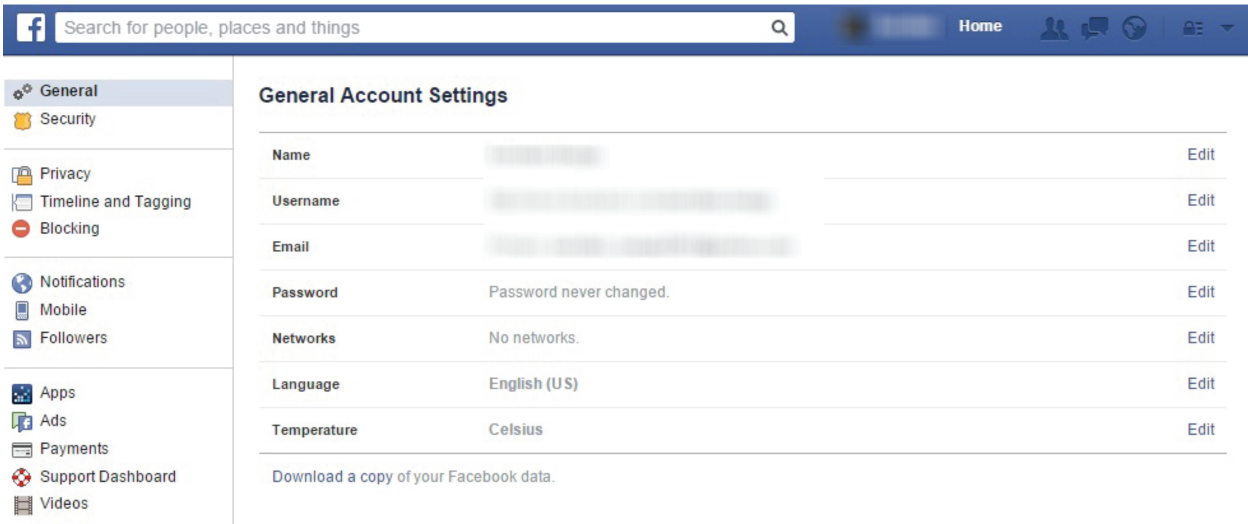
To access your Facebook account settings, start by going to the top right corner of your screen and select **Settings** from the drop-down menu.



Note: Though I can classify actions and steps in **security** and **privacy** sections, I believe it is easier for you to follow me, as I take each section and discuss it before I continue to the next, **as it appears in the Facebook settings menu.**

General Account Settings

By clicking the **Settings** button, you should see the **General Account Settings** on the left hand side of the page in the provided sidebar.



General Account Settings

Name	[redacted]	Edit
Username	[redacted]	Edit
Email	[redacted]	Edit
Password	Password never changed.	Edit
Networks	No networks.	Edit
Language	English (US)	Edit
Temperature	Celsius	Edit

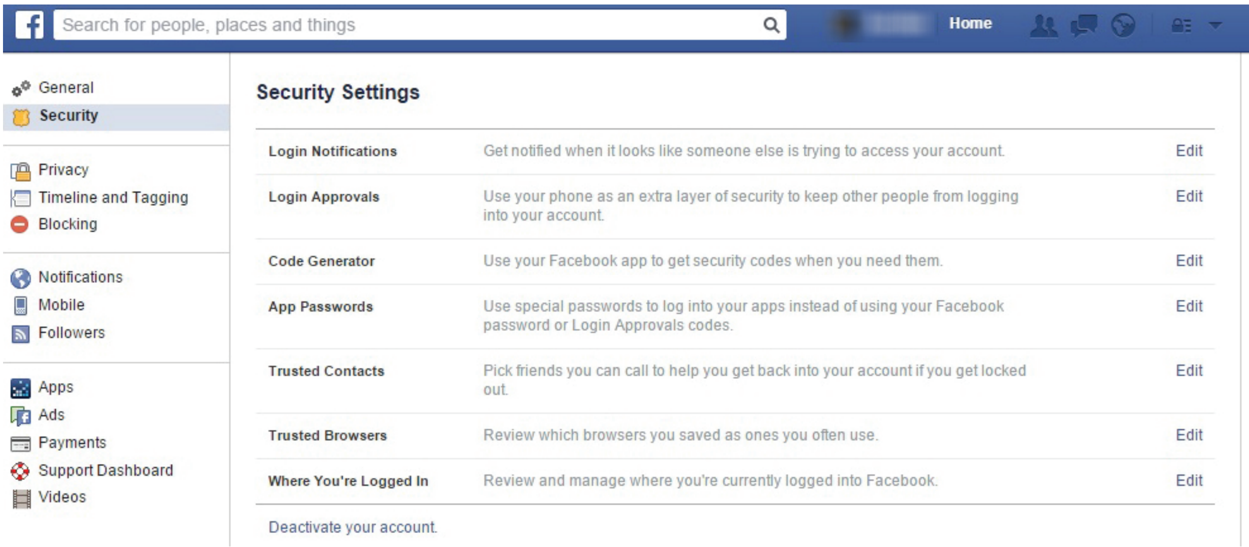
Download a copy of your Facebook data.

In this location you can update your Facebook account password and **Download a copy of your Facebook data.**

Lesson 13

Security Settings

Let’s continue on the left hand side of the page with the **Security Settings**.



Security Settings

Login Notifications	Get notified when it looks like someone else is trying to access your account.	Edit
Login Approvals	Use your phone as an extra layer of security to keep other people from logging into your account.	Edit
Code Generator	Use your Facebook app to get security codes when you need them.	Edit
App Passwords	Use special passwords to log into your apps instead of using your Facebook password or Login Approvals codes.	Edit
Trusted Contacts	Pick friends you can call to help you get back into your account if you get locked out.	Edit
Trusted Browsers	Review which browsers you saved as ones you often use.	Edit
Where You're Logged In	Review and manage where you're currently logged into Facebook.	Edit

Deactivate your account.

Login Notifications

This option allows you to opt in to receive **Text and Email messages** when your account is accessed from an unknown computer or mobile device. This is very useful in case a hacker tries to access your account.

Login Approvals

Turning on this option will require a security code to be generated in order to access the account on a new browser. You have three options:

- have a security code sent by **SMS** to your mobile device;
- generate a security code by **Code Generator** in your Facebook mobile device app, if you have an Internet connection;
- pre-generate **10 codes that you can print** on a piece of paper and use them when you don't have your phone with you;

This layer of security is also meant to keep other people from accessing your Facebook account.

Code Generator

This option is used with **Login Approvals** to create codes that you can use to access your Facebook account from a new browser.

App Passwords

This option helps you create single use passwords to access third party applications on Facebook and keep your main Facebook password safe. When you log out of the application, the password is not saved. To access the third party application again, you will need to generate a new password.

Trusted Contacts

Select close friends to contact if you have any trouble accessing your Facebook account.

Trusted Browsers

This is where you find a list of saved (trusted) web browsers you used to access your Facebook account. You can choose to remove a browser from the list if you don't use it anymore, let's say you left your work place and of course, you don't use the browser in that location anymore.

Where You're Logged In

This is where you can review your logged-in status and End Activity (terminate the session) on places and devices you don't recognize.

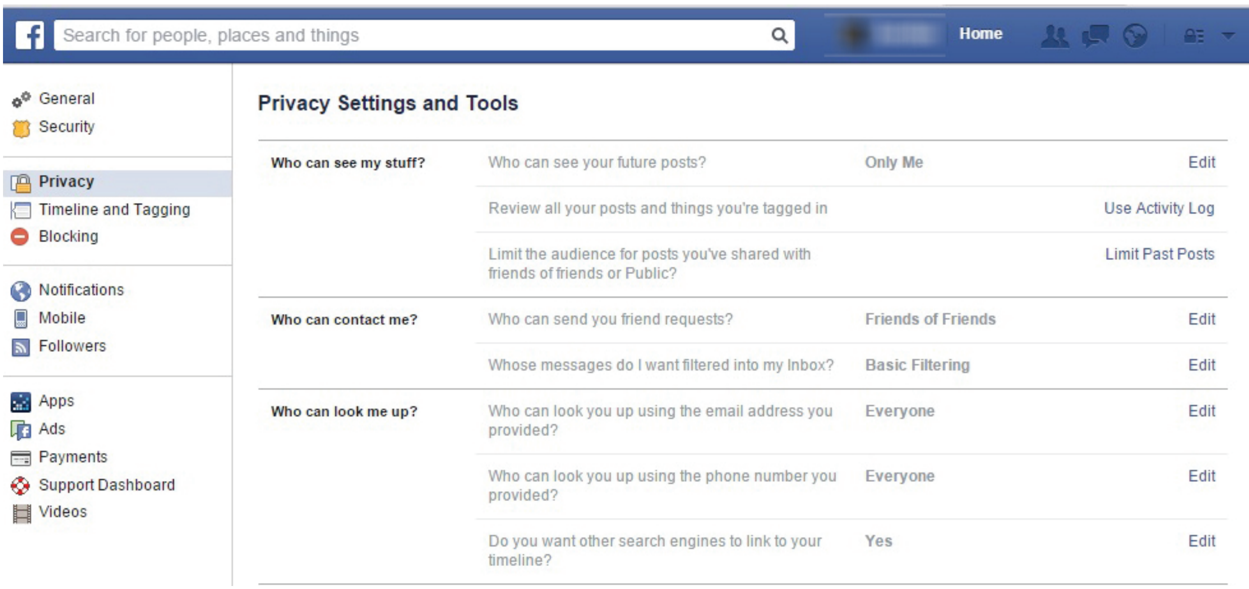
Deactivate your account

From this place, you can choose to deactivate the Facebook account. This is useful if you know that you won't be able to access, or you simply don't want to access, the Facebook account for a period of time. You can reactivate the account at any time.

Lesson 13

Privacy Settings

The next section you need to access to improve your overall security is the **Privacy Settings** area. The settings from this location are meant to help you review **basic privacy settings** and make sure your profile and the content you shared are viewed by the **audience** you select.



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Only Me	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of Friends	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	Yes	Edit

Who can see my stuff?

Select the **audience** for your posts. You can choose:

- Public
- Friends
- Friends with Acquaintances
- Only Me
- or you can create a Custom audience

I recommend you to set the default sharing option to **Friends**.

In the same location, you can review your posts and your Facebook activity by using the Activity Log, or limit the audience for your posts in the past.

Who can contact me?

Set who can send you friend requests. If you want to be located by people you used to know in the past, you need to set this to **Everyone**.

Who can look me up?

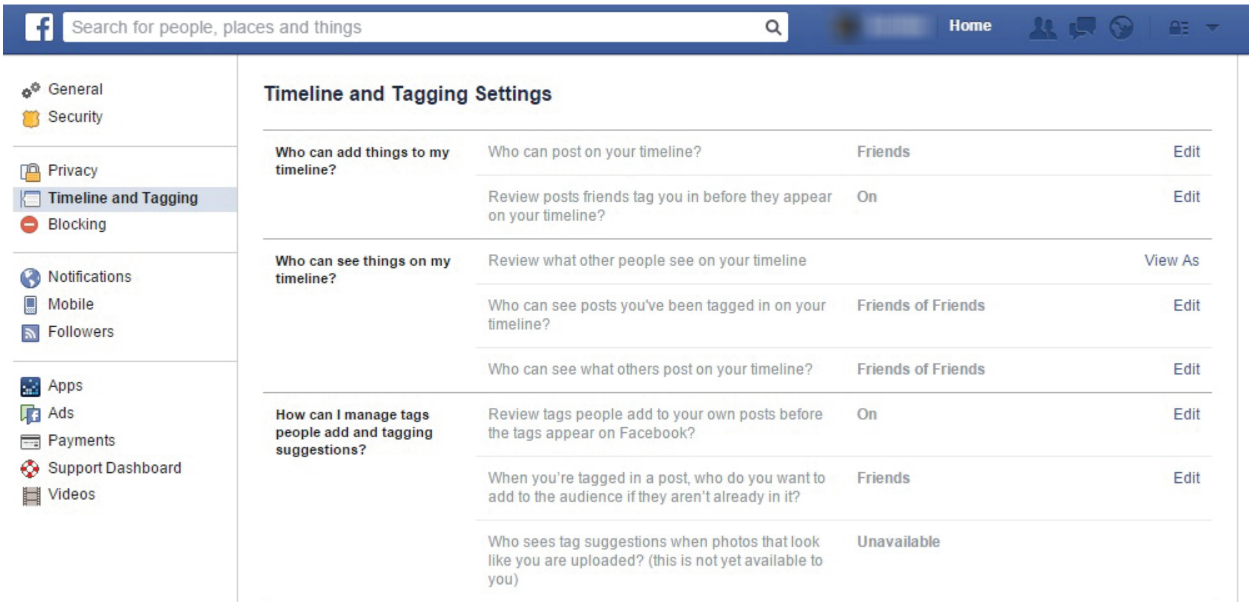
In this place, you can choose if you want to be looked up by people using your **email address** or your **phone number**. At the same time, you can select if you want **search engines** to send someone looking for your name to your **Facebook timeline**.

This is an important privacy setting that you should consider, since your Facebook timeline will appear in search engine results if someone searches for your name.

Lesson 13

Timeline and Tagging Settings

This place allows you to set other **privacy settings** for your Facebook account. You can choose who can **add things to your timeline**, **who can see posts** you share on your timeline and how to manage tagging options.



Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends of Friends	Edit
	Who can see what others post on your timeline?	Friends of Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

Who can add things to my timeline?

This one is pretty straight forward. You can choose to allow friends posting on your timeline and review a post you are tagged in, before it appears online.

Who can see things on my timeline?

Use this option to **check what other people have access to on your timeline.** You can select a single person and view how he or she views your timeline. You can also select who can see posts you have been tagged in on your timeline and choose who can see what others post on your timeline. In the last two cases, you should set these options to **Friends**.

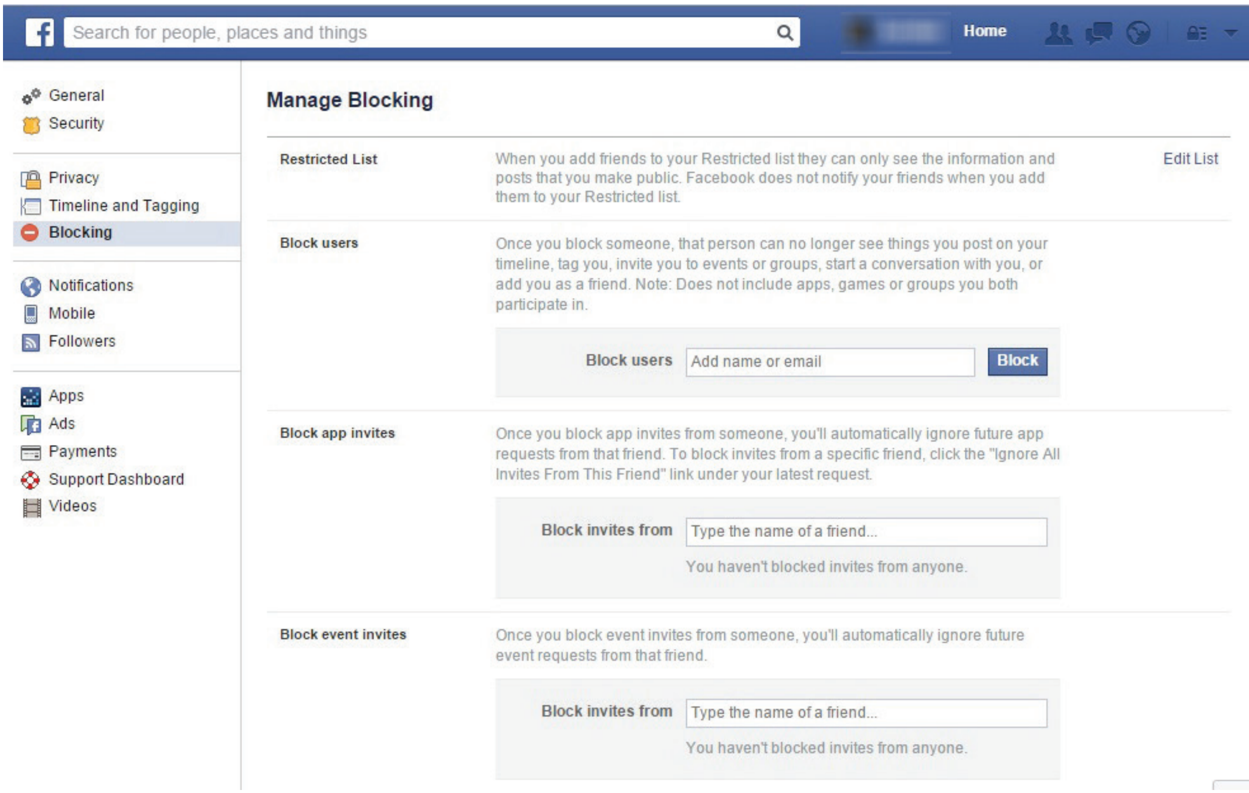
How can I manage tags people add and tagging suggestions?

Turning on this option, you will be able to **check the tags friends add to your photos** before they appear. It is an important privacy option because if someone adds a tag to one of your posts, his/her entire list of friends will see your specific post.

Lesson 13

Blocking

In the Blocking tab you can restrict the way in which other Facebook users, Facebook applications or pages interact with you.



Manage Blocking

Restricted List: When you add friends to your Restricted list they can only see the information and posts that you make public. Facebook does not notify your friends when you add them to your Restricted list.

Block users: Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users: Add name or email

Block app invites: Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request.

Block invites from: Type the name of a friend...

You haven't blocked invites from anyone.

Block event invites: Once you block event invites from someone, you'll automatically ignore future event requests from that friend.

Block invites from: Type the name of a friend...

You haven't blocked invites from anyone.

Restricted List

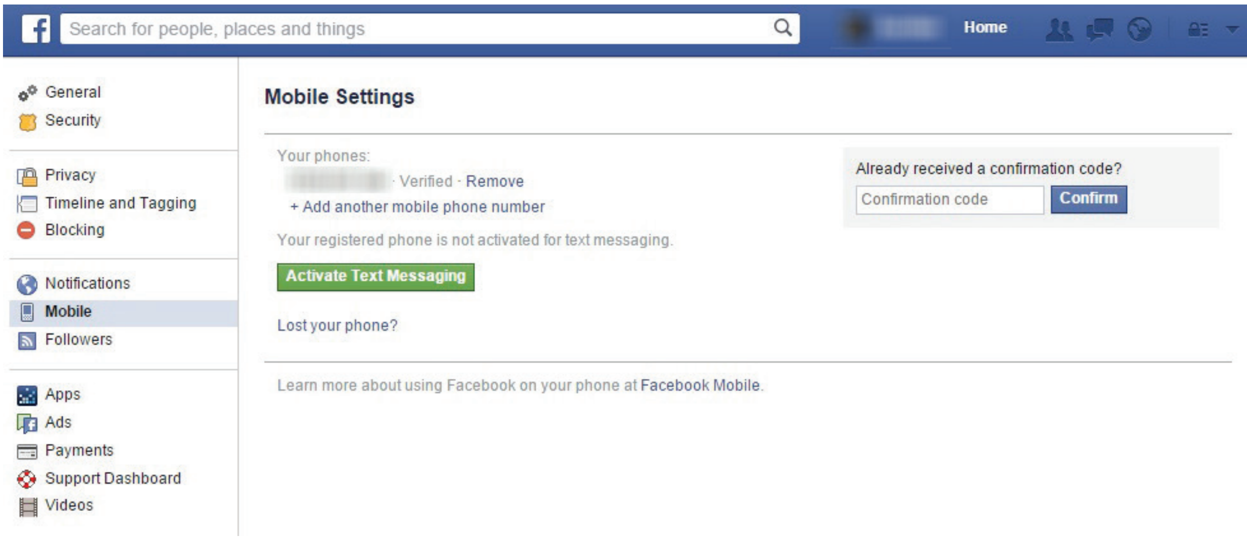
This list is useful when you want to restrict a friend from seeing the posts you share on your timeline for other friends. Nevertheless, that person can still see content you make public.

Block users

Users you add to this list cannot see your Facebook profile, send you invitations, add you as a friend or start a conversation with you. Use this option to add a friend whose account has been hacked. In the same Blocking tab, you have the option to block app invites or event invites from someone, block apps and Facebook pages.

Mobile

This is probably one of the most important security settings you can set to your Facebook profile.



Mobile Settings

Your phones:
[redacted] · Verified · Remove
+ Add another mobile phone number

Your registered phone is not activated for text messaging.

Activate Text Messaging

Lost your phone?

Already received a confirmation code?
Confirmation code | Confirm

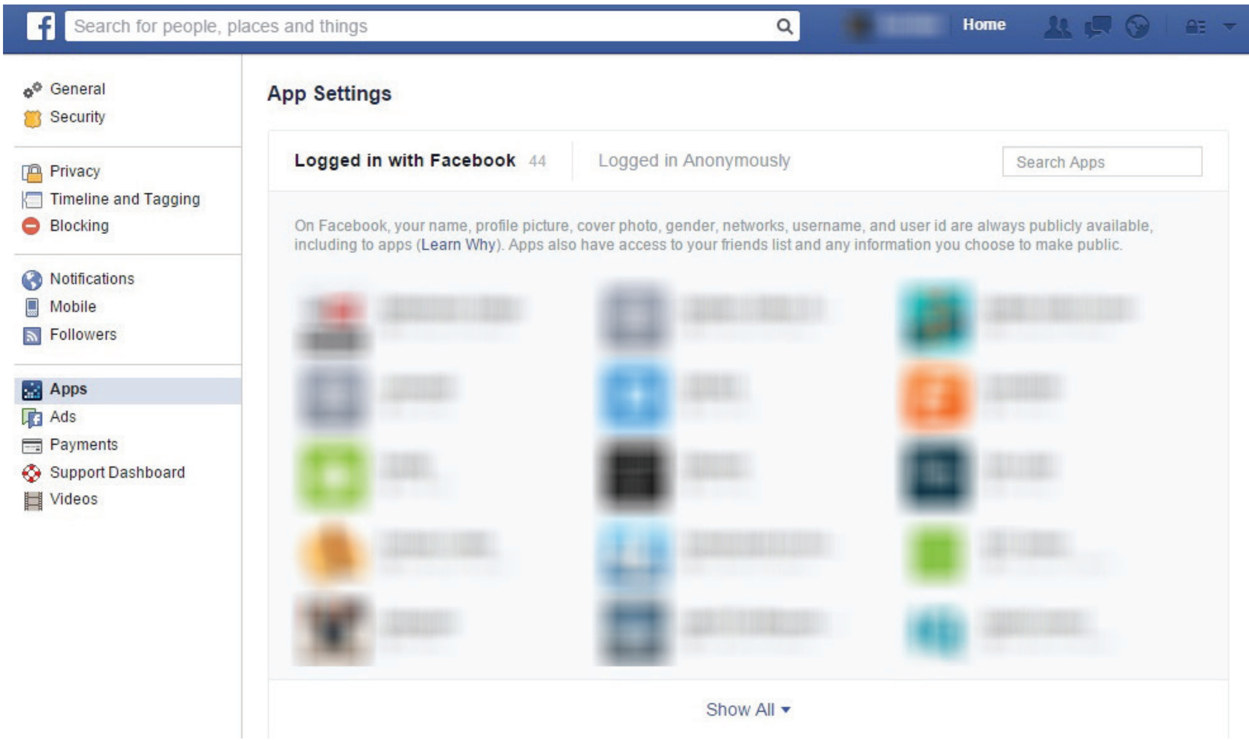
Learn more about using Facebook on your phone at Facebook Mobile.

To enable **Login Approvals**, you need to enter a mobile phone number here. In case your browser is not recognized, you will receive a code via text message to log in to your Facebook account.

Lesson 13

Apps

Most of us use third party applications on Facebook, applications which usually ask permission to access our content and private data.

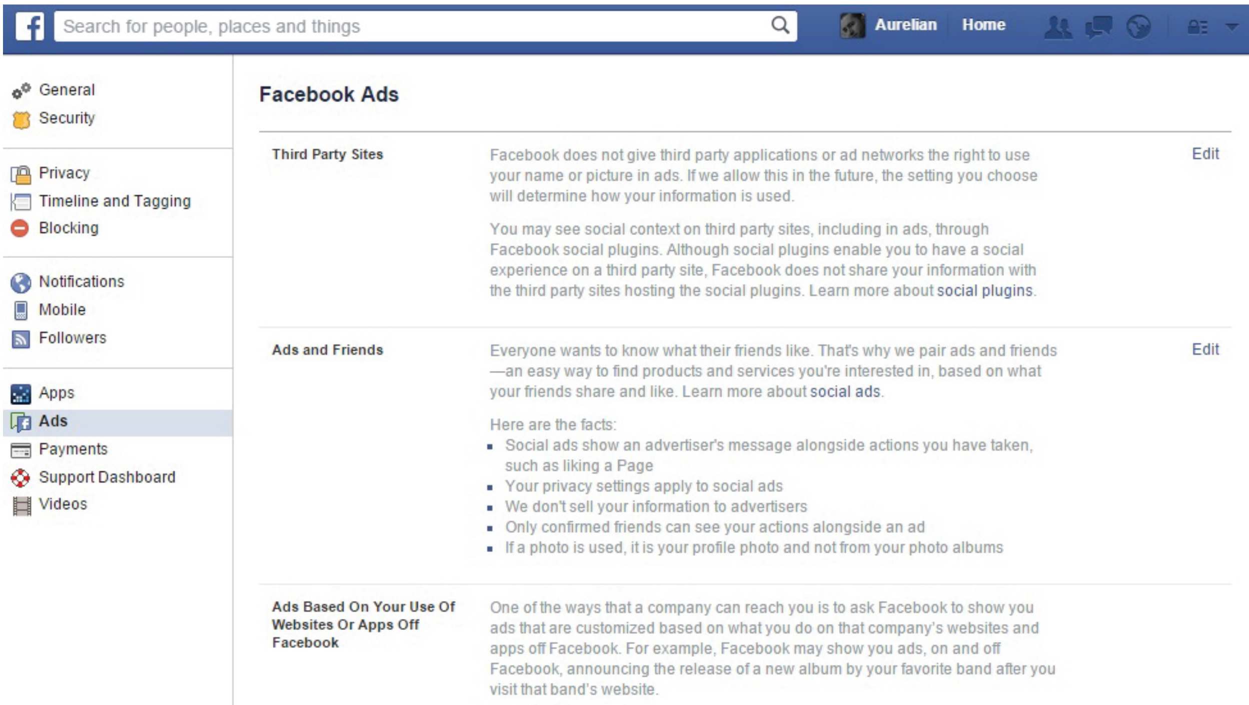


On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps (Learn Why). Apps also have access to your friends list and any information you choose to make public.

In this location you can see exactly what each third party app has access to and you can choose to remove it from the list, in case you don’t use it anymore or you have discovered you are dealing with a suspicious app.

Lesson 13

Ads



Facebook Ads

Third Party Sites — Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used.

You may see social context on third party sites, including in ads, through Facebook social plugins. Although social plugins enable you to have a social experience on a third party site, Facebook does not share your information with the third party sites hosting the social plugins. Learn more about social plugins. Edit

Ads and Friends — Everyone wants to know what their friends like. That's why we pair ads and friends —an easy way to find products and services you're interested in, based on what your friends share and like. Learn more about social ads. Edit

Here are the facts:

- Social ads show an advertiser's message alongside actions you have taken, such as liking a Page
- Your privacy settings apply to social ads
- We don't sell your information to advertisers
- Only confirmed friends can see your actions alongside an ad
- If a photo is used, it is your profile photo and not from your photo albums

Ads Based On Your Use Of Websites Or Apps Off Facebook — One of the ways that a company can reach you is to ask Facebook to show you ads that are customized based on what you do on that company's websites and apps off Facebook. For example, Facebook may show you ads, on and off Facebook, announcing the release of a new album by your favorite band after you visit that band's website.

Do you want to allow **third party sites** access to your personal information?

Do you want Facebook telling your friends what you like? If you want to opt-out from these two options, simply select **No one** to these two options.

The third option, **Ads based on your use of websites or apps off Facebook**, let's you opt out of ads that are selected for you by Facebook, based on your behavior on a particular website. We all searched for a hotel on a website and we were amazed to see on our Facebook page an ad for that hotel.

10 tips and tricks for increasing your Facebook security

1. **Don't accept friend requests from unknown people.** One of the favorite methods used by online scammers to collect private data and sensitive information from users is by creating fake Facebook profiles. Make sure you and your children pay attention to this possible privacy threat.

2. **Do not disclose your personal details and your Facebook credentials** (email address, phone number and password) to other users. This information can be used by cyber-criminals to access your personal data.

3. **Keep your browser up-to-date with the latest available patches.** Your browser and other software on your system, not to forget the operating system, should have the latest patches installed. Stay safe and don't expose your system to cyber-criminal attacks.

4. **Use a good security program.** You need to rely on a good security software, which includes a real-time scanning engine. This means that files you download from online locations are analyzed in a very short period of time.

5. **Stay safe from phishing attacks.** Pay attention to the various messages you receive from unknown users, which ask for your personal data.

6. **Don’t use the same password from your Facebook account to other online accounts.** If you use the same password in other locations as well, you are vulnerable to a potential hacker attempt that tries to get access to all your accounts.

7. **Activate Login Approvals.** Though I have already mentioned this step before, I need to emphasize again its importance.

8. **Be careful when connecting to free wireless networks from public spaces.** Online criminals use these types of unprotected networks to access users’ credentials and steal sensitive data. To limit your exposure, you can use a **private browsing** session.

9. **Don’t click that link!** Since social media and in this case, our Facebook profile, is used for spreading and sharing various content, it is also one of the favorite means of carrying malicious links across the Internet.

10. **Log out of your Facebook account.** This piece of advice is useful when using a public or work computer, which is used by multiple individuals.

Lesson 13

Protect your Twitter Account in 10 Steps

Twitter is one of those popular social media platforms used not only by private individuals, but by large businesses and important names in the IT industry.

Due to its short writing style, it has been related to journalism and even used as a **favorite news spreading tool for revolutions and revolts around the world.**
To stay safe from malicious attacks targeting social media accounts and prevent online criminals from retrieving private data from us, you need to follow additional steps to keep your Twitter account secure:

1. Create and use a strong password

Yes, I know, it is easy to remember and use a password in multiple online accounts. Maybe using something familiar like your family name or your birthday date seems to be a good idea. **But isn't this exactly the same thing online criminals count on?**

To make sure your account is safe from online intrusions, it's key to create a strong password which includes upper and lower case characters, numbers and symbols, and is over 10 characters long. This way it will be difficult for cyber-criminals to access your Twitter account.

At the same time, don't use the same password in more than one online account. The reason is easy to guess: if one of your online accounts is hacked, the others will soon follow. By using different passwords, you reduce the potential loss in case your Twitter account is accessed.

2. Use login verification

Login verification is a security option which helps you protect your Twitter account.

It is **a form of two-factor authentication**, where you'll be asked to provide a phone number and an email address before you connect to your online account.
This login verification adds a second check, where you have the following 3 options:

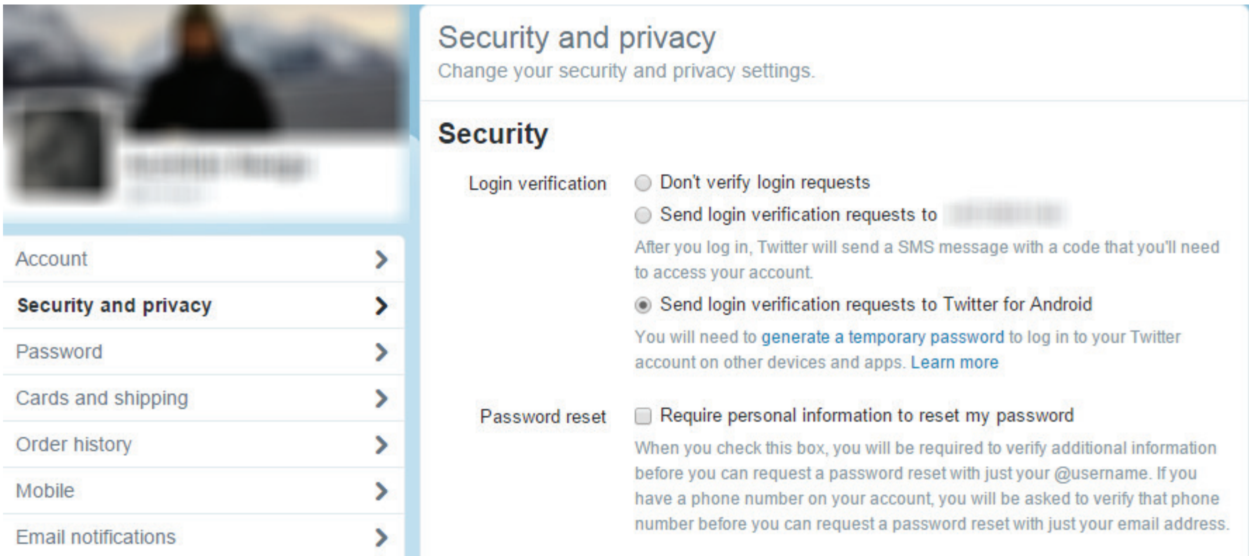
- enter a verification code sent to your phone's Twitter app
- enter a text message sent to your phone number
- enter a photo of a backup code saved on your phone from when you first enrolled in login verification

To activate Login verification, follow these steps:

1. Access your Twitter account.
2. Go to the top right corner and click your user image.
3. Choose **Settings** from the drop down list.

Lesson 13

4. Click **Security and privacy** in the left menu.
5. Select the corresponding option.



[redacted]

- Account
- **Security and privacy**
- Password
- Cards and shipping
- Order history
- Mobile
- Email notifications

Security and privacy

Change your security and privacy settings.

Security

Login verification
○ Don't verify login requests
○ Send login verification requests to [redacted]
After you log in, Twitter will send a SMS message with a code that you'll need to access your account.
● Send login verification requests to Twitter for Android
You will need to generate a temporary password to log in to your Twitter account on other devices and apps. Learn more

Password reset
□ Require personal information to reset my password
When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

3. Don't post private information and do not disclose your location

Don't let online criminals know where you are and what you're doing. By default, Twitter is a public network and anyone and see your tweets and can follow you.

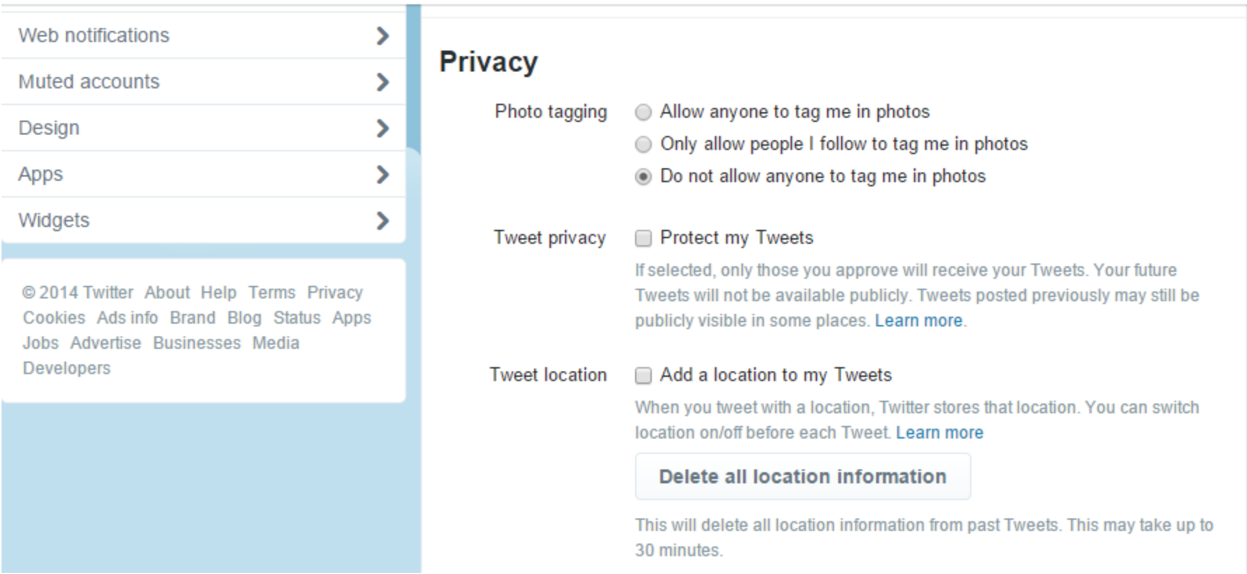
If you want to control other people's follow requests or you want to share your tweets only with your followers, you can make the necessary modification in the **Security and privacy** area and check **Protect my Tweets** under the Privacy section.

At the same time, make sure you **don't offer valuable**

information to cyber-criminals, such as your **location**. This kind of data becomes very important for a hacker who wants access to your private files or needs to create a persona for you, in order to proceed to identity theft attacks.

To protect your tweets and disable tweets location, follow these steps:

1. Access your Twitter account.
2. Go to the top right corner and click your user image.
3. Choose **Settings** from the drop down list.
4. Click **Security and privacy** in the left menu.
5. Select the corresponding options.


Web notifications
Muted accounts
Design
Apps
Widgets
© 2014 Twitter About Help Terms Privacy Cookies Ads info Brand Blog Status Apps Jobs Advertise Businesses Media Developers

Privacy

Photo tagging
○ Allow anyone to tag me in photos
○ Only allow people I follow to tag me in photos
● Do not allow anyone to tag me in photos

Tweet privacy
□ Protect my Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location
□ Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

Delete all location information

This will delete all location information from past Tweets. This may take up to 30 minutes.

4. Stay safe from phishing attempts

Phishing attempts on Twitter usually start with **a direct message you receive** from an unknown person who tries to retrieve your Twitter credentials for spamming purposes.

It is a classic **phishing attack** through which they try to trick you into giving away **personal information or private data.**

This type of message will provide a link, which sends you to a malicious login page. Don't reply to this type of email or click the provided link.
At the same time, many of us had that Twitter friend which sent an unusual direct message to all his followers. In this case, that particular account has been hijacked and you should not reply or click any link that it may contain.

5. Use a specialized security solution against spyware threats

Even if you pay attention to phishing attempts and spam campaigns, you still need to keep yourself secured with a **safety net**. I am talking about a specialized security solution against spyware threats.

To keep your system secured against spyware, use one of the popular **anti-spyware products** available online. A few security solutions capable of removing spyware from your system are Malwarebytes, Spybot Search and Destroy, Lavasoft's Ad-Aware, etc.

6. **Check what apps can access your Twitter account**

Another important way to protect your account is to **be cautious when giving access to third-party apps** — these services can gain full control of our account.

To make sure your Twitter account is not vulnerable, do not give access to **untrusted third party apps**. When you give your account credentials to an app, they have complete control and they can take actions which may cause your account to be suspended.

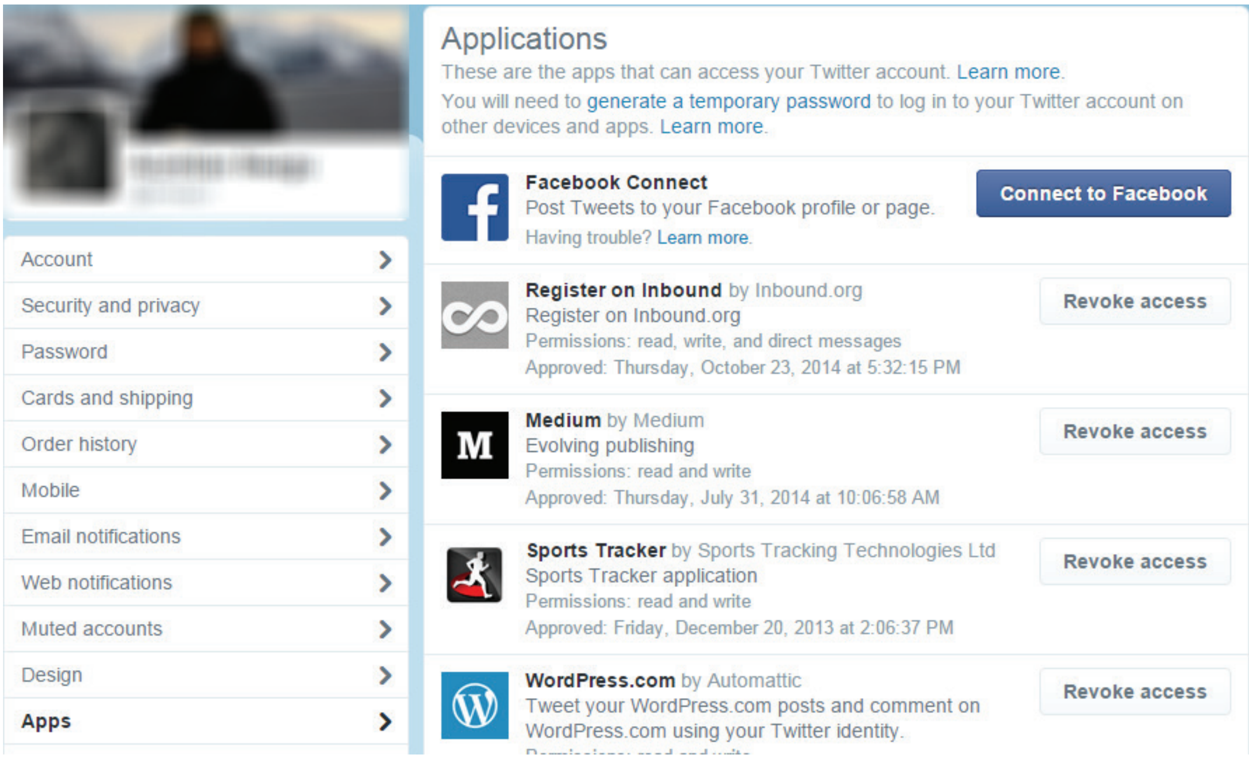
Pay extra attention to apps that promise money or a big number of followers. When in doubt, simply search the Internet for that app's name before you provide access.

To check permissions apps have to your Twitter account, follow these steps:

1. Access your Twitter account.
2. Go to the top right corner and click your user image.
3. Choose **Settings** from the drop down list.

Lesson 13

4. Click **Apps** in the left menu.
5. Take the necessary steps to allow or revoke access.



Applications

These are the apps that can access your Twitter account. Learn more.

You will need to generate a temporary password to log in to your Twitter account on other devices and apps. Learn more.

Facebook Connect
Post Tweets to your Facebook profile or page.
Having trouble? Learn more.

Register on Inbound by Inbound.org
Register on Inbound.org
Permissions: read, write, and direct messages
Approved: Thursday, October 23, 2014 at 5:32:15 PM

Medium by Medium
Evolving publishing
Permissions: read and write
Approved: Thursday, July 31, 2014 at 10:06:58 AM

Sports Tracker by Sports Tracking Technologies Ltd
Sports Tracker application
Permissions: read and write
Approved: Friday, December 20, 2013 at 2:06:37 PM

WordPress.com by Automattic
Tweet your WordPress.com posts and comment on WordPress.com using your Twitter identity.

7. Make sure you keep your vulnerable apps up-to-date

Security news on software vulnerabilities have appeared lately all over the important security blogs and related IT channels in the industry.
These threats cannot be ignored. **Cyber-criminals use software vulnerabilities** in our systems and mobile phones apps to take advantage of our private data and use it in identity theft attacks.

Therefore, keeping popular software like Java, Adobe

Flash, Adobe Shockwave, Adobe Acrobat Reader, Quicktime up to date is important, but
paying attention to our **mobile phones apps** is also important and you should always make sure you have the latest updates installed.

8. Use a Virtual Private Network to Hide Your IP Address

One of the favorite methods used by cyber-criminals to steal credentials is to employ **wireless sniffers** to retrieve data sent over unsecured networks.

To safeguard your social media accounts and protect your online activities, you can use a **VPN**, that is a Virtual Private Network.

Using a VPN means that you **hide your IP address**, encrypt your connection and access various web locations in a **private environment**. This method keeps your sensitive data from cyber-crime, identity theft and phishing attempts. Stay safe online especially when using wireless networks by using a popular VPN like CyberGhost.

9. Secure your browsing habits

Choose your web browser with care and make sure you have made the necessary changes to improve your security and privacy. Vulnerabilities in web browsers are **like**

open doors to hackers, who try to retrieve private data from our systems and from our social media accounts.

To secure our online privacy, follow these guidelines:

- Secure your web browser from online criminals' attacks by choosing the latest version for your browser and installing the latest security patches.
- Read this Ultimate Guide to Secure your online browsing and increase your online security
- If you access your social media account from an unsafe location, choose a **private browsing session** in order to remove the browsing history details.

10. Don't forget to log out from your Twitter account

This security step should be followed if you connect to your account on a **public computer**. Though you may be used to closing the web browser as soon as you are done with your activity, you should **remember to log out** from your accounts when you finish your online sessions.

If you don't do this, especially if you are in a public location, the next person who opens the Twitter account, for example, will access directly our online profile.

Private browsing sessions are also recommended if you want to prevent authentication credentials (or cookies) from being stored.

Protect your LinkedIn Account in 10 Steps

Social media is not all about having fun. Or starting a revolution for that matter.
You may go for Twitter if you want to find out the latest news and choose Facebook to stay up-to-date with your friends' latest interests.

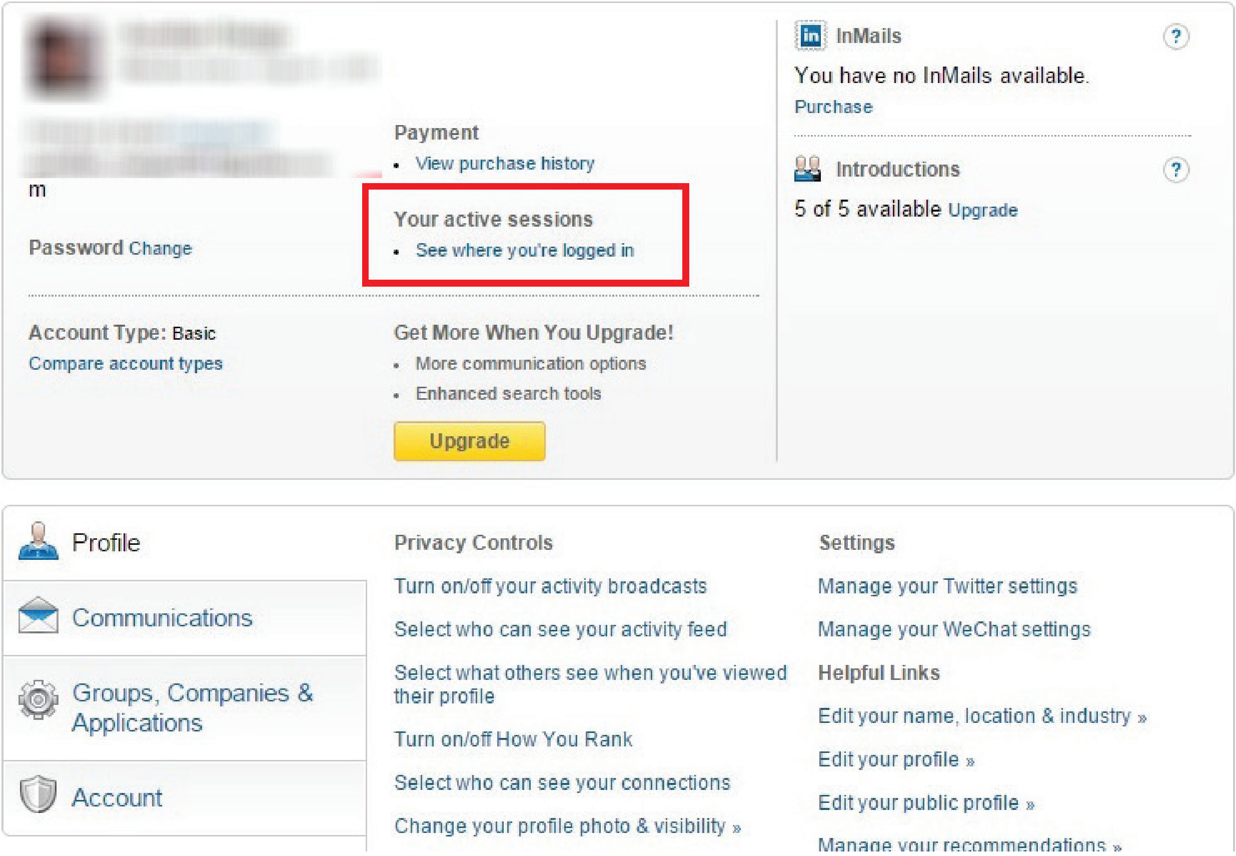
But when you turn to your **LinkedIn account**, you need to keep things **serious and professional**. And this is even more important than on the other less "serious" channels.

LinkedIn can become our vulnerability when dealing with online criminals, since there is **more private information shared publicly** than on other popular social media accounts. You simply **expose and reveal more about ourselves** than on our Facebook profile.

Therefore, make sure you follow these 10 steps in order to increase your security when using your LinkedIn online account:

1. **Check your current connections to LinkedIn**

Lesson 13



[redacted]

m

Password Change

Payment
- View purchase history

Your active sessions
- See where you're logged in

Account Type: Basic
Compare account types

Get More When You Upgrade!
- More communication options
- Enhanced search tools

InMails
You have no InMails available.
Purchase

Introductions
5 of 5 available Upgrade

Privacy Controls
Turn on/off your activity broadcasts
Select who can see your activity feed
Select what others see when you've viewed their profile
Turn on/off How You Rank
Select who can see your connections
Change your profile photo & visibility »

Settings
Manage your Twitter settings
Manage your WeChat settings

Helpful Links
Edit your name, location & industry »
Edit your profile »
Edit your public profile »
Manage your recommendations »

This option is very useful because it allows you to see which devices you have connected to your LinkedIn account and which sessions are still opened.

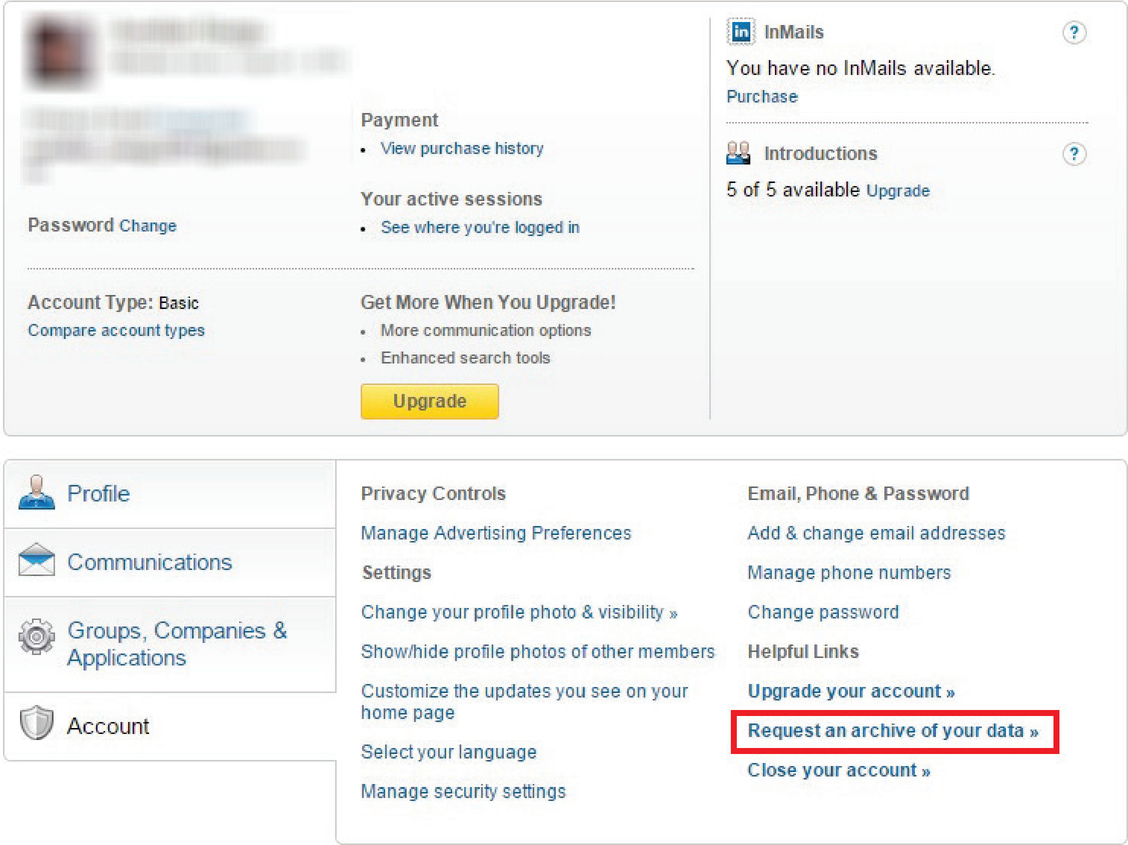
This LinkedIn feature can help you if you know you have connected to your LinkedIn account from a publicly shared computer or from a computer in a place you have recently left.

In case you notice you are connected to your online account from an unknown device, choose the option to sign out as soon as possible from that device.

Lesson 13

It may be a cyber-criminal trying to retrieve sensitive data from your account and using this private information later on against you in an identity theft attempt.

2. Request an archive of your data



Password Change

Payment
- View purchase history

Your active sessions
- See where you're logged in

InMails ?
You have no InMails available.
Purchase

Introductions ?
5 of 5 available Upgrade

Account Type: Basic
Compare account types

Get More When You Upgrade!
- More communication options
- Enhanced search tools

Upgrade

Profile
Communications
Groups, Companies & Applications
Account

Privacy Controls
Manage Advertising Preferences
Settings
Change your profile photo & visibility »
Show/hide profile photos of other members
Customize the updates you see on your home page
Select your language
Manage security settings

Email, Phone & Password
Add & change email addresses
Manage phone numbers
Change password
Helpful Links
Upgrade your account »
Request an archive of your data »
Close your account »

Using this option, you can request LinkedIn to send you **an archive of your account data.**

It is an important step for your online privacy allowing you to see not only what information you made available online for others, but IP records of your past login connections, recent searches and other details.

3. **Who do you connect to?**

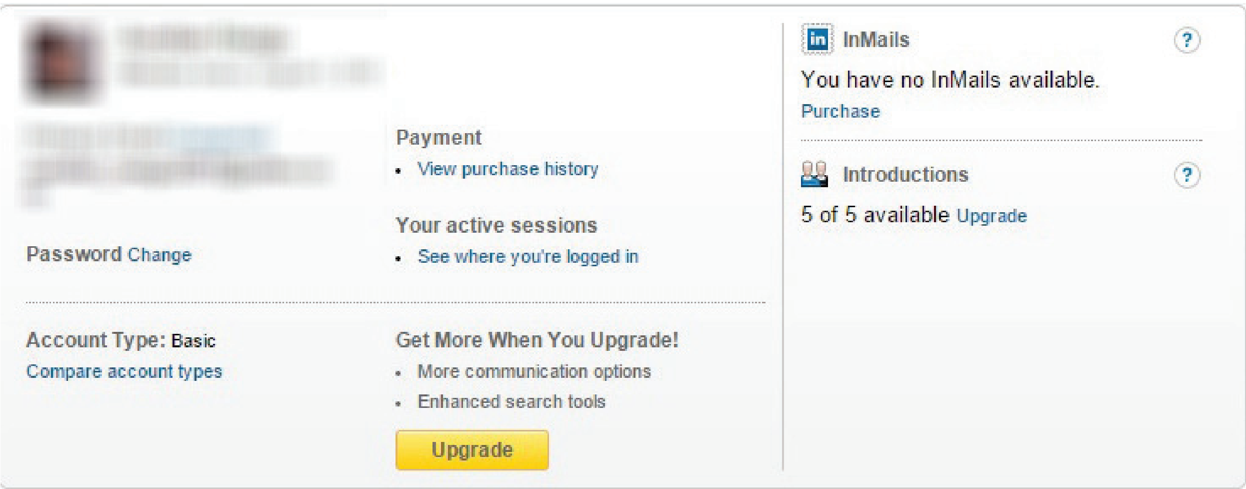
   Connect only to people you know and trust. Adding to your list of connections unknown people, or people you don't actually know very well, increases the risk of adding online criminals who only want to use your personal information.
   Using this professional data, which can be combined with personal information from social media accounts, like Facebook, cyber-criminals attempt to put all this data together before they run an **identity theft operation.**

   Before you know, your online banking accounts' credentials have been guessed and your money removed without any notice.

   We have dedicated **lesson 4** to this topic.

4. **Let's keep it private: protect your sensitive information**

Lesson 13



[redacted]

Password Change

Payment

- View purchase history

Your active sessions

- See where you're logged in

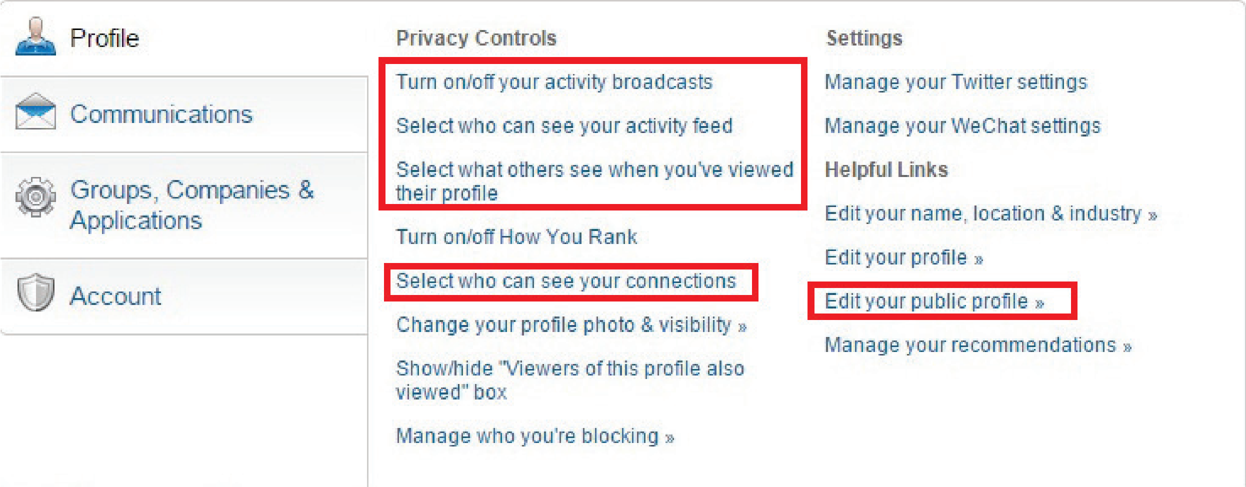
Account Type: Basic
Compare account types

Get More When You Upgrade!

- More communication options
- Enhanced search tools

InMails
You have no InMails available.
Purchase

Introductions
5 of 5 available Upgrade



Privacy Controls

Turn on/off your activity broadcasts
Select who can see your activity feed
Select what others see when you've viewed their profile
Turn on/off How You Rank
Select who can see your connections
Change your profile photo & visibility »
Show/hide "Viewers of this profile also viewed" box
Manage who you're blocking »

Settings

Manage your Twitter settings
Manage your WeChat settings

Helpful Links

Edit your name, location & industry »
Edit your profile »
Edit your public profile »
Manage your recommendations »

Online security is connected to privacy. As I mentioned above, private information may be used against you if it comes in the wrong hands. Therefore, you need to pay attention to what you share with others, **especially with unknown people you have given access to your LinkedIn profile.**

Use the following options to increase your privacy online:

- **Turn on/off your activity broadcasts:** If you want to hide from your connections the changes you choose to do on your profile, who you follow or when you make recommendations, choose to uncheck this option.

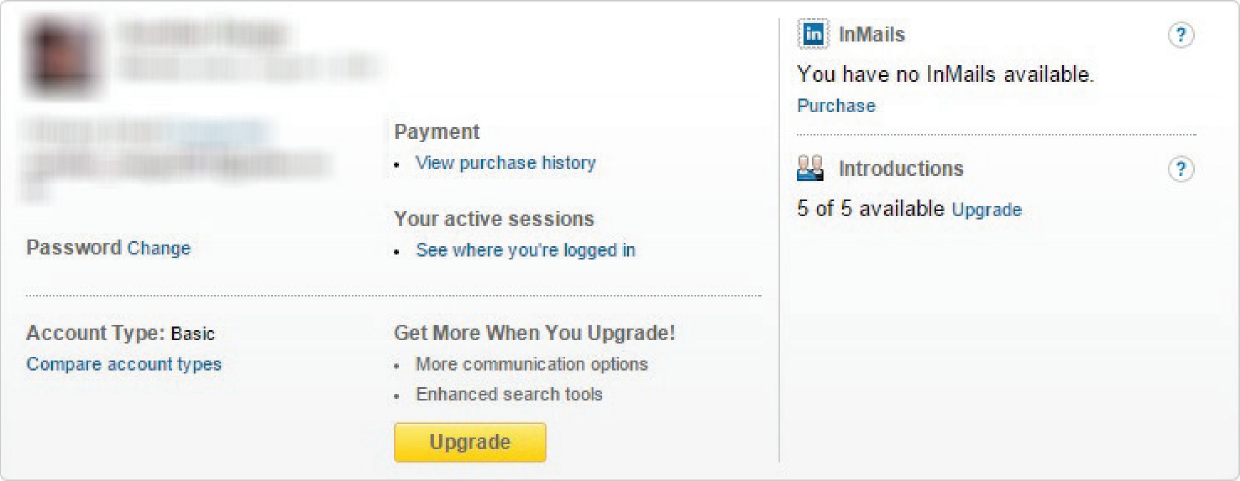
- **Select who can see your activity feed:** To hide your actions on LinkedIn or let only some connections see your actions, select from the drop-down menu: **Everyone, Your network, Your connections** or **Only you.**

- **Select what others see when you've viewed their profile:** You don't want your connections see that you accessed their LinkedIn profile? Choose to go **anonymous** using this option.

- **Select who can see your connections:** You don't want to share your list of connections with the others in the list? Use this option to change it to **Only you**.

- **Edit your public profile:** How do other people see you? Did you know you can control your public profile and how you appear on search engines? This is the place where you can make the necessary modifications and what information **you choose to make visible online**, like your current or past work places, your skills or your education. **Choose wisely.**

5. Enable Two-Step Verification to block cyber-criminals from accessing your online account



[redacted]

Password Change

Payment
- View purchase history

Your active sessions
- See where you're logged in

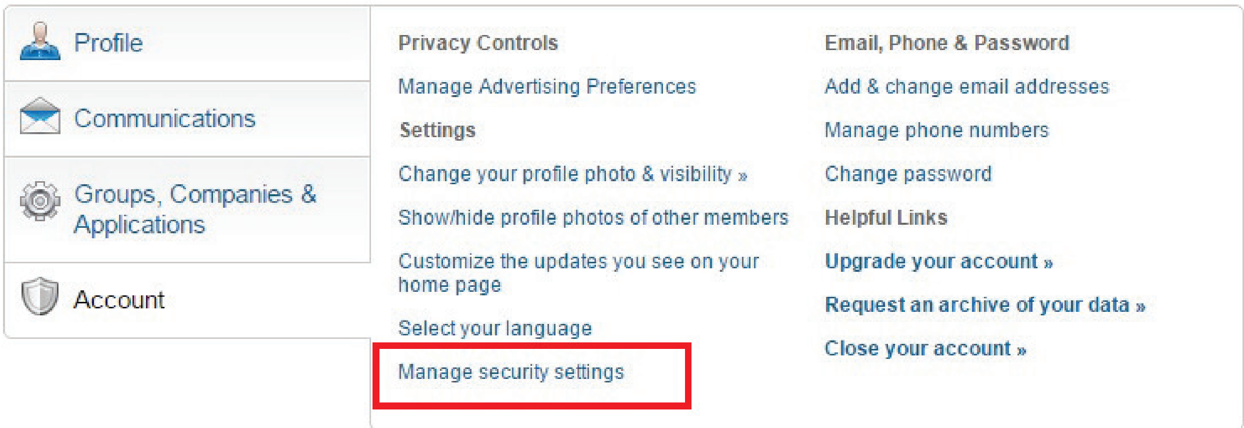
Account Type: Basic
Compare account types

Get More When You Upgrade!
- More communication options
- Enhanced search tools

Upgrade

InMails
You have no InMails available.
Purchase

Introductions
5 of 5 available Upgrade



Profile
Communications
Groups, Companies & Applications
Account

Privacy Controls
Manage Advertising Preferences
Settings
Change your profile photo & visibility »
Show/hide profile photos of other members
Customize the updates you see on your home page
Select your language
Manage security settings

Email, Phone & Password
Add & change email addresses
Manage phone numbers
Change password
Helpful Links
Upgrade your account »
Request an archive of your data »
Close your account »

First of all, I need to say that this security measure should be enabled and used for any online account you have, where this option is available. Some of the most popular online accounts allow activating this security step, for example Google, Facebook, yahoo Mail or Dropbox, to name a few.

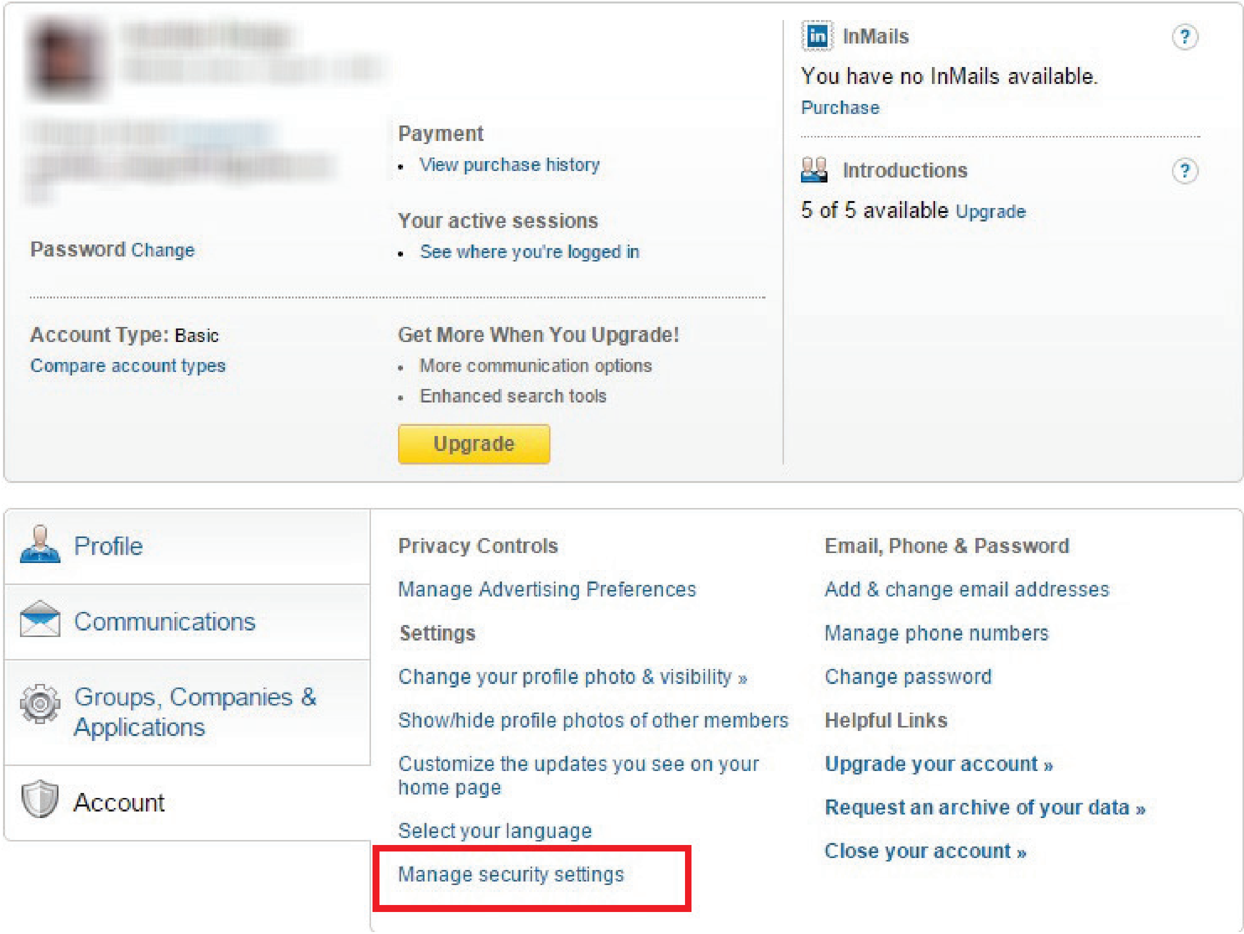
But what exactly is Two-Step Verification for LinkedIn?

Lesson 13

This security option is a form of verification that **can be used against identity theft and unauthorized access to your LinkedIn online account.**

Activating Two-Step Verification requires that you insert **a security code sent to your phone** every time you connect from an unknown device. Since most cyber-criminal attacks and identity theft attempts occur from unknown devices, I strongly recommend using this security option.

6. Secure your connection with HTTPS option



Password Change

Payment
- View purchase history

Your active sessions
- See where you're logged in

Account Type: Basic
Compare account types

Get More When You Upgrade!
- More communication options
- Enhanced search tools

Upgrade

InMails
You have no InMails available.
Purchase

Introductions
5 of 5 available Upgrade

Profile
Communications
Groups, Companies & Applications
Account

Privacy Controls
Manage Advertising Preferences

Settings
Change your profile photo & visibility »
Show/hide profile photos of other members
Customize the updates you see on your home page
Select your language
Manage security settings

Email, Phone & Password
Add & change email addresses
Manage phone numbers
Change password

Helpful Links
Upgrade your account »
Request an archive of your data »
Close your account »

Using the same location in the LinkedIn security settings where you enabled Two-Step Verification, you have the option to activate the secure browsing mode.

This security option should be used as an **extra protection step against unauthorized access to your browsing sessions** and to make sure you are actually connected to your real LinkedIn account.

Most of all, I recommend activating and using this secure browsing option **if you access LinkedIn regularly from unsafe or public locations, such as Wi-Fi networks in cafes, airports or hotels.** These places are usually favorite locations for online criminals to access and retrieve your online accounts' credentials for banking websites and other online accounts.

7. Don't forget to sign out of your online account

This is something I highly recommend, especially after using a publicly shared computer or an unsafe Wi-Fi network. We tend to think that closing the web browser as soon as we are done with our online activity is enough, but **you should remember to log out every time you finish your online connection.**

If you forget to do this, especially if you are in a public space, **any person accessing the browser may be sent**

directly to your online profile.

At the same time, if you really need to use a computer from a public location and you are not sure about its security settings, I recommend using a **"private browsing"** session, which prevents your browsing session history and credentials from being preserved.

8. **Keep your software up to date**

   Software vulnerabilities seem to increase each day. Now, they have become **one of the main tools used by online criminals** to take advantage of our systems.

   By not keeping our Windows operating system and our programs up-to-date, you allow online criminals to use these security gaps and gain access to your programs and applications. It is a quite well known fact that vulnerable software applications like **Java, Adobe Flash, Adobe Shockwave, Adobe Acrobat Reader, Quicktime** are on most people's computers and are **widely used**.

   Few people in return actually acknowledge **these solutions are under threat from cyber-criminals** and they should use a dedicated solution to keep them up-to-date.

9. **Set a Strong Password for your LinkedIn account**

You may notice by now that **I recommend more than anything setting a strong password**, if you have an online account. So, the same advice is valid here.

Here are a few simple steps you can follow:

- Use **different passwords** for different online accounts. In case one of your online accounts is accessed by an IT criminal, at least you know that the other online accounts won't follow.
- Make sure your password has over 10 characters.
- Don't forget to use capital letters, numbers and symbols.
- Use a special program to keep your passwords, like LastPass.

*Remember **lesson 4**, when we helped you make your passwords hacker-proof?*

10. Watch out for phishing messages requesting personal or sensitive information

Phishing is an old tactic used by IT criminals who try to **steal your sensitive information and your financial data.** For this reason, you should keep an eye, not only on email messages, but also on messages received via your LinkedIn account.

For this reason, always look closely at the received email before you open any attachment or click any link in the message. Do you know the sender or the company who send the message? If you are not sure about their identity, look them up online for more information.

Do they ask you to download and install an application? This is not a good sign of trusting that message. And is there a link you need to follow? **Check the link before you click it**. Simply hover the mouse over the link to see if it sends you in a legitimate location. To make sure you are going in a good direction, check the suspicious links using a reliable URL checker, such as **VirusTotal**.

I know it was a long guide to follow, but you can access and use only the necessary steps for your favorite social media platform.

I know it's hard not to click that link, like or share your friends' photos or stop your mother for liking your every photo! But while you have fun online on these networks, inventing or reinventing our lives, you must not forget about security.

Lesson 14 /19

“Nobody understands the cloud!” - is that you? How to keep your cloud-stored data safe

Lesson 14

In today’s tech-dominated environment, we keep trying to find software that will make us more productive, more creative, more organized and, especially, more relaxed.

So we try a lot of new services, because they seem interesting, because they promise us we’ll have more time to spend doing the things we love.

The problem is that **we rarely think of the security implications** every new app we begin using brings to our lives. And to think it used to be so simple…

Do you remember how your personal IT “infrastructure” used to look like 7-8 years ago?

Just like me, you probably had a desktop computer or had just bought your first laptop, which relied on a dial-up connection or on a really poor DSL one. Smartphones were practically dinosaurs compared to what we use today!

But progress is not only necessary for our evolution, but it’s also exciting! Today, our personal IT micro-universe looks more like a piece of corporate infrastructure, with tenths of services relying upon each other to handle our data and make it accessible everywhere.

I wonder if you were as skeptical as me when you first hear about “the cloud”.

Remember this scene from the movie “Sex Tape”?

Lesson 14

https://www.youtube.com/watch?v=ecZL4Q2EVuY

That's how I used to feel about services like Dropbox, Google Drive and so on. But since then I've learnt a few tips & tricks to keep my cloud-stored data safe, and today I want to share them with you!

Lesson 14

The unique security challenges of cloud computing

I bet you don't want to be one of those people who says that *"nobody understands the cloud!"* So here are some of the **dangers that threaten your cloud-stored data:**

- Unauthorized access,
- Data loss and data leakage,
- Loss of control and many more cyber security risks can be listed.

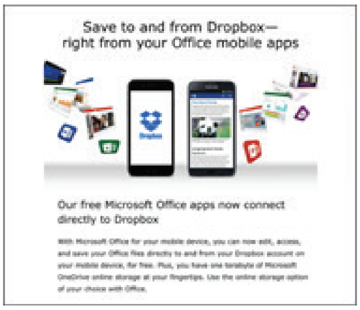
And there are various **ways in which cyber criminals can break into your cloud apps or services**, to list a few:

- **By breaking your password.**
- **By using an insecure API** (APIs are the building blocks used for building software). For example, if you have your Facebook account connected to Dropbox, so it can automatically save the picture you post, if your Facebook account gets compromised, the same will happen to your Dropbox account.
  Cloud apps usually plug into one another, so if one account gets compromised, so do all of the others who are connected to it. Just look at some of the many integration options that Dropbox offers:

Lesson 14

Keep your photos safe with Dropbox

Copy 3,187 photos from iPhoto to Dropbox.
Dropbox will create a new folder for each of your 58 events.



Save to and from Dropbox—
right from your Office mobile apps

Our free Microsoft Office apps now connect directly to Dropbox

With Microsoft Office for your mobile device, you can now edit, access, and save your Office files directly to and from your Dropbox account on your mobile device, for free. Plus, you have one terabyte of Microsoft OneDrive online storage at your fingertips. Use the online storage option of your choice with Office.

- **By persuading you into uploading a malicious file to your cloud account**, which could provide the cyber criminal with the tools he needs to gain control over your cloud account and delete everything that’s in there. Yes, that could also include your back-up.

- **By using access to your data to leak it to third parties.** For example, if you share a folder with someone, and that person has malicious intentions, he/she could use the occasion to leak your data to cyber criminals. Or if that person’s account gets compromised, your account could suffer the same fate.

Should I give up using cloud apps?

Definitely not! You just have to **ensure adequate protection.**

8 GOLDEN RULES TO PROTECT YOUR CLOUD ACCOUNTS

1. **Learn how to create strong passwords and how to safely manage them**, so you'll never have to worry that a cyber criminal can barge right into your accounts. Oh, and don't EVER store a list of passwords in a text file, in your cloud account! Waaay back in lesson 4 I put together a password security guide that is always useful to revisit.

2. **Keep it clean and simple:** do a general check-up of your cloud accounts, and see what services depend upon another. If you haven't used that specific dependency in the last 2 months, it's probably time to revoke access for that app to your cloud account.

3. **Beware of social engineering** and its consequences.

4. **Use next-generation anti-hacking tools** along with your antivirus solution (which is not quite enough nowadays). If you go back to lesson 6 you'll find out more about the crucial role that these tools play in your cyber protection system.

5. **Sharing is caring** – when you do it safely. See who are the people who have access to documents stored in your cloud account and take the necessary actions: revoke access where no longer needed and limit access to "read

only" where possible. You should refrain from offering administrator privileges to anyone, even if you trust them. If their account gets compromised, yours can become liable as well.

6. **Back-up your data in several places** (a cloud account + an external drive). It's always a good idea to keep multiple back-ups of your data, in case anything should happen to one of them. Go back to lesson 8 for a full, easy to apply guide on data back-ups.

7. **Encrypt your data!** It may sound like encryption is only for hardcore security fans, but that's just a misconception. Encryption has many benefits and we dedicated lesson 10 to a dedicated encryption guide that you can apply to protect your data.

8. **Strengthen your Wi-fi security.** Do you use a Wi-fi connection most of the time? When you're at work, you'll most likely connect to a secured hotspot, but you should take additional precautions at home as well. And if youre tempted to use a public Wi-fi hotspot, then it could come in handy to go over lesson 11 again for valuable tips 7 tricks!

When it comes to security, remember that **it all works together:** technology depends on the human factor to make it work, but it can also be compromised by the same thing.

Dependencies are essential when you think about how all the services we use work together, so be careful how much access you give to apps into your private information.

Coming up in the next lesson (number 15):

Do you know where your data is?

We’ll teach you all about blocking identity theft attempts like a Pro! Take that, cyber criminals!

Lesson 15 /19

Where is your data? Block identity theft attempts like a Pro

I am sure this won't come as a surprise for you or anyone else:

Malicious software and cybercriminal tricks **ARE REAL** and affect us all.

But the worst malware types that could hit us, like advanced pieces of data stealing malware or ransomware threats, they usually stop at our computers.

Identity theft is something much worse.

Identity theft happens when an individual (it may be a hacker or a cybercriminal), steals your private information – usually financial data – and assumes your identity, while running data stealing operations or financial transactions in your name.

The reason why it's so difficult to protect yourself from this is because most times you find out too late, when police arrives at your door holding you responsible for various financial crimes developed in your name.

Therefore, you are not dealing with a simple crime, but with an advanced scheme that targets your valuable financial details and your personal information.

In case you are affected by identity theft, contact police as soon as possible.

But, as they say, it's better safe than sorry, so make sure you follow the steps below to protect from **online and physical threats**.

Lesson 15

Fend off cyber threats like a PRO!

1. **Choose a good strong password for your online accounts**

   This step is a classical one, but it cannot be avoided. Passwords are only as good as the encrypting programs that are used to protect valuable information.
   Just remember to make sure your passwords incorporate uppercase and lowercase letters and numbers, and are more than 15 characters long.

   Credentials for online accounts should not be easy to access by a potential hacker, so it is recommended to use a password manager as LastPass.

   *Remember **lesson 4**?* I won't go anymore in details.

2. **Protect your computer with multiple security products**

   Identity thieves use multiple tools to get to your personal data. I am not talking about the classical viruses here, I refer to advanced malware and spyware tools that are capable to retrieve sensitive information from a system without the user's knowledge.

   These advanced pieces of malware are designed to evade the normal antivirus detection and sometimes a long time passes until the user becomes aware of their presence.

*Do you remember **lessons 5 and 6** where we talked about antivirus products and additional security protection?*

3. ***Are you using a specialized security solution against financial and data stealing malware?***

   Traditional security solutions may not be able to fight advanced pieces of code developed by cyber-criminal minds.

   To ensure financial security for banking operations and protection against Zero Day malware, you need an advanced scanning technology that can protect you from the latest threats.

4. ***Are you keeping your operating system safe from spyware?***

   Do you really want pop-up windows, malicious locations and spyware tools all over your system?
   To stay safe from spyware, use one of the popular anti-spyware products available online. A few security solu-

tions capable of removing spyware from your system are Malwarebytes, Spybot Search and Destroy, Lavasoft's Ad-Aware, etc.

5. ***Could you spot an online phishing scam if it targeted you?***

How to prevent identity theft from online criminals that target sensitive information and use various tools and methods has always been a difficult task to accomplish. Using all sorts of weapons, from traditional attack vectors to phishing scams, these individuals seem impossible to catch.

The main phishing schemes and campaigns appear when:

- you shop online
- you check our email account
- access social media networks

As you can see, your online presence and activity is targeted by cybercriminals because their main target is YOUR MONEY.

Though phishing schemes use multiple channels and methods to retrieve our sensitive credentials and attempt identity theft, **the email spam campaign is still the**

number one method used to target user's credentials and steal identity details.
Therefore, make sure you don't answer unwanted mail from unknown sources and keep your antivirus real-time protection enabled, in case you access such an email or its content.

6. ***Do you shop online?***

Of course you do! And I bet you love it too!

But do you know how to detect a fake website that wants to steal your money?
Follow these steps and make sure you don't send your financial details to cybercriminals:

- *Do you know the website you're shopping from? Is it the first time you're using it? **How did you discover the site?***

- *Did you check the security symbols or any sign of legitimacy on the website, like the lock icon encryption?* At the same time, check the address starts with **"https://"**. The **"S"** is from "secure socket layer" and you know you are going to a site where communication is encrypted. If you don't want checking all the time the web address, use HTTPS Everywhere. This extension has the role to encrypt your communications with many major websites, making your browsing more secure and safe from online criminals.

- *Are you unsure about a website? Why don't you check it out on search engines or on the **Trustpilot** site?*

- If you purchase online often and from different locations, I recommend that you use a secondary card for online shopping. In case something bad happens, you still have the **"good card"**, which is usually the one you are using to receive the monthly salary or run important transactions on safe websites.

7. Don't post confidential information online

What you publish online stays there for a long period of time and it's available for everyone to see. So, pay attention to personal data you place in comments, posts or the pictures you display on your social media networks.

Even more, you need to teach your children or your parents that online actions have real consequences and using credit cards on any website poses serious privacy risks that could lead cybercriminals to launch identity theft operations.

8. Keep your system and software up-to-date

Keep your system up-to-date with the latest security patches available. The same thing you should do for your vulnerable applications and programs.

Patches for a program or application are delivered by the vendors to cover any security hole that may appear in a software program, like Java, Adobe Flash or the popular web browsers.

If you don't want to bother checking and keeping the vulnerable applications up-to-date every day, I recommend using a free dedicated solution to do the job.

9. Secure your browser settings

Our browser is the tool we use to connect to most websites that we are interested in and to the online places where we run financial transactions.
For this reason, an important degree of attention needs to be given to our web browser, and the following guidelines should be followed:

- Are you using the latest version for your browser? Make sure you have the last browser version that contains all the available security patches.

- Improve your browser's security settings.

- Use a **private browsing session if you connect from a public computer.** You don't want your browsing history details to be recorded locally. To hide your online connection, go online and search for a **free proxy server**. Use the proxy to connect to any website and make sure your IP address has been hidden from any online surveillance mechanism.

- To bulletproof your online activity and hide all the important financial and personal details from any type of surveillance, you can **encrypt your online connection by using a VPN software or Tor browser** that hides your browsing activity by routing your traffic through the Tor network of computers.

10. How much do you share on Facebook?

There is no discussion that social media has become an important part of our lives. Nowadays every friend, work colleague or family member has a Facebook account.

It is the place where you can find almost any individual and this leads to an increasing danger for your personal information, since in this common space the distinction between public and private is blurred and what is private data becomes public knowledge.

How much do you share?

Physical Threats – what can you do about those?

The steps you can follow to remain hidden from identity theft attempts suppose more than online protection. For this reason, I will continue to present **the measures that protect your physical identity from theft attempts.**

11. *Who's watching you?*

You are in front of an ATM machine or at the local shop and try to withdraw some money or just insert your PIN to pay.

Did you consider hiding your personal identification numbers or your bank account details from a possible privacy breach?

Before placing your sensitive data, look around and make sure there's no one looking suspicious or who stays too close to see your information.

Even if you don't see anyone around, there may still be **thieves that use special surveillance mechanisms or simple binoculars to look from a distance.** Another possibility is to use hidden cameras, so just to make sure you are on the safe side, try to hide the numbers you insert.

12. *What do you carry with you?*

So many times you go out for a walk or for a dinner in the evening. Maybe you go to see a friend or just watch a new movie at the cinema.

Do you really need to carry with you all the credit cards and your official papers?

Before you leave your home, just think a bit if you need all those things with you and take only the necessary. You need to do this because in case you lose or forget them somewhere, you limit the potential loss.

At the same time, these days many banks offer a second authentication measure when paying online: you can set a password or receive a final identification code on your phone before you place the order.

If you really need to carry your valuable credit cards, your ID or maybe your passport, where are you keeping them? How do you carry them around?
To limit the potential loss, follow these steps:

- **Don't leave your bag unattended in a public place** or place it far from you. If a thief takes your bag, can you catch him in time? Should you?

- **Don't leave your wallet** or purse in a jacket just hanging around. Don't make things easy for the thief.

- Imagine that your wallet or bag have been stolen. How much did you lose? What are the actions you need to take to retrieve your official papers? **Do you have the bank phone number to call for a potential block?** Follow this step especially when you are located in a remote place or have left in a long travel.

- Consider distraction elements for the thieves. **Keep a fake wallet** or don't place important things in the bag that can be stolen. Keep the important stuff with you.

13. Destroy any documents or papers you don't need anymore

I am sure you keep important data in your home, like information from past work places, medical records, certifications and diplomas from school and university, maybe sensitive information if you run a business.
But, along this information **you have the tendency to collect various papers and pieces of information that you**

don't actually need anymore, like receipts or bank statements.

Though you may not need that data anymore, it doesn't mean that for someone else, it is not an important element that might be used to reach valuable financial details we have hidden.

14. Protect your normal mail box

Just think like an identity thief.

You need to find personal information, especially financial details about someone. *How do you do it? Where do you start from?*

We think the easiest way is to start with those areas that are less protected, like the mail box. And now that you know where they will attack, just think about it:

- ***What type of information do you receive in the mail box?*** *Do you receive important documents from the bank, maybe the next credit card?* If you do, you need to contact the bank and have them stop this type of correspondence. If you have important stuff you need to collect from the bank, just go to the bank.

- ***Do you receive invoices for every service in the house?*** Maybe it doesn't seem like too much data for you, but an identity thief can use this information to correlate it to other sources in order to have an image on your financial situation. Wouldn't it be easier to receive the invoices by email, since today most services providers offer this option.

- ***How well did you secure your mail box?*** If anyone can access your mailbox and you know that vital information is delivered there, probably you should get a high security locking mailbox or a personal one in the post office.

15. Do you know who's calling?

Yes, an identity thief may call you, posing as a bank agent or official representative and ask for private details or financial data.

How does the thief know what's your bank? Remember the previous points? Is it really that hard to obtain this information?

They may look through your mail box, they may watch you at the shop or at the ATM or they may even look through your garbage. It is not difficult to discover this piece of information.

And don't be fooled by the professional tone they use or the fact that you're talking to a nice woman. This criminal profession knows no limits. Therefore, do not provide important information over the phone, unless you initiated the phone call and you really know who you're talking to.

16. Destroy your digital information

How many CDs and DVDs have you collected along the years?
And sometimes, you have been forced to throw into thrash a hard disk which didn't seem to work anymore, without thinking about the private data we have left there.

To understand how the information from an abandoned disk can harm you, just think about all the photos, documents and private details you have left there.

Using special tools and software, a hacker who finds such a disk can retrieve all that information easily and use it against you.

To make sure that an insecure disposal of old disks doesn't become an opportunity for identity thieves, you need to destroy that data.

The following options are available:

- Overwrite the data a few times and make things a bit more difficult for an identity thief.
- **Physically destroy that hard disk or that DVD. Smash it. Crack it. Bust it to smithereens!**
- *Did you know printers and photocopiers also have hard disk built in?* So, don't just throw away that printer before removing the hard disk first.

17. Protect your Social Security number

This is one of the most important steps you need to take to protect your identity from thieves, since this piece of information can be used in multiple situations.

Using your social security number an identity thief can apply for a new credit card or open a bank account.

It can also be used to obtain access to ask for a loan or rent a house. Or it can be used to prove your identity over the phone or online in order to access private information.

Here are a few techniques you can use to protect it:

- Don’t use it as a password on any online account.
- **Don’t just take it with you anywhere, unless you really need it.**
- Don’t send it over the email.
- Don’t store it on your computer, your smartphone or your cloud drive.

18. Keep your smartphone safe

How many things are you doing by using only your smartphone?

I am sure you already forgot those things are for calling someone. We all use our smartphones to take pictures, use various apps, have direct access to our cloud drive or even run financial transactions.

And this becomes our greatest risk. Just think about the amount of information one gets access to, just by having access to our smartphone.

That’s why, I have to underline a few steps that need to be followed in order to improve our smartphone’s data doesn’t fall into the wrong hands:

- Download apps from well-known companies, especially apps that are used for financial transactions.

- Physically watch your smartphone and instruct your children on this too. Just by gaining access to your smartphone, an identity thief obtains a large amount of information.

- Secure the mobile device with a strong password or better yet, use 2 methods to keep it sealed from any breach.

- Use the best apps available to protect your smartphone. Most of them include a GPS feature and a remote wipe out mechanism.

19. Check your bank account transactions every month

You think you know what purchases you have operated that month, but sometimes cybercriminals find ways to steal just a small amount of money in order to test your attention.

There are so many cases where customers' credit card information has been "read" and used in restaurants and stores, only to find out later about this, when it was already too late.
A good idea is to **activate on your bank account the option to receive alerts** for any sum of money that has

been retrieved.

And make sure you know the **bank's policy** on this type of cases, so that you know what's next if your card is under attack.

20. Back it up

I don't mean the computer back-up now, but **the idea of backing something up is to accept that a certain thing may be lost at some moment.**

Let's try to answer a few questions so that we may solve this problem:

- *Are you keeping all your money on one credit card?* ***Why?*** Just use at least 2 and split the money.

- *Do you carry both cards with you when you go out?* ***Why?*** Just take one or at least, don't place them both in the same place. Limit the potential loss.

- *Do you need to verify your identity somewhere?* Ok, **take an identification paper or document with you, but don't take the ID, the driver license and the passport along.**

- *And do you really need an official document with you?*

Maybe you can replace it with a photocopy. In any case, make sure you always have photocopies for all the important documents, especially when travelling.

- *Do you have a phone number where you can call for help in case you lose an official paper or the credit card?*

We did our best to cover any possible situation that may appear, from online threats developed by cybercriminals to physical threats that appear when you carry important documents, like identification papers or your smartphone.

Once identity theft occurs, it is difficult to recover personal data or any piece of information cyber-criminals have stolen. This happens because many times you don't know how and when it happened.

The idea behind all this is simple: **Always be ready for every possible situation.**

It is better to prevent cyber-criminals from stealing banking details and personal information than take measures when it may already be too late and your money have been retrieved.

Lesson 16 /19

Are you under attack? Detect & block cyber criminals actions

Lesson 16

We talked about online security and how you can be safe from online threats that affect us, *but can YOU learn how to detect malware?*

With so many ways out there to access and exploit vulnerable systems, **I want to make sure you are able to recognize a malware infection** in order to defend your systems from malicious software and cybercriminals.

For this reason, **you need to find out how a malware infection appears,** so that you can correctly assess the risk and create an effective defense strategy.

10 Warning Signs That Your Computer is Infected

1. Slowdown

It takes longer than normal for your operating system to boot up? *Are you waiting too long for some of your programs to start?*

We all know that **malware** has the tendency to **slow down** your operating system, your Internet speed or the speed of your applications.

If you notice something like this and you are not using any resource-heavy program or application, check first for other causes. It may be a lack of RAM memory, a fragmented system and a lack of space on your hard drive or maybe a hardware issue affecting your drive.

If you have already verified these possible causes and all seemed fine, maybe you should start suspecting a malware issue on the system.

2. Pop-ups

One of the most annoying signs of malware is represented by the unwanted pop-up windows. Unexpected pop-ups that appear on the system are a typical sign of a spyware infection.

In this particular case, the main issue is created not only by the numerous pop-up windows that affect your Internet navigation, but also because it is quite difficult to remove them from the system. Pop-ups are not only annoying, but they usually come together with other malware threats which are concealed from your eyes, and which could be far more destructive for your systems.

To avoid spyware and its negative consequences for our systems, keep in mind a few security practices:

- don’t click any suspicious pop-up windows
- don’t answer to unexpected answers

- be careful when downloading free applications

To remove this type of threat, you need a very good security product against spyware. A few popular products capable of removing spyware from your system are **Malwarebytes, Spybot Search and Destroy, Lavasoft's Ad-Aware** and others.

3. Crashes

If your programs or your system regularly crash or the infamous *BSOD (Blue Screen of Death)* appears regularly, it is a clear warning that your system is not working properly and you should look into it.

I need to mention here the 2 particular cases which may cause this problem:

1. You could be dealing with a technical issue caused by a potential incompatibility between your programs or it may be a malware issue. If you suspect a technical issue, multiple software problems may lead to this. ***Are you running various programs which may conflict with each other?*** *Is there any orphan registry keys which have not been removed slowing down and eventually crashing your system?*

2. If you are checking for malware, simply run a complete scan on the system with a good antivirus product. **It is important to have a reliable security solution on your system,** which should include real-time scanning, automatic update and a firewall. *Do you remember lesson 4, where we talked about choosing a good antivirus product?*

4. Suspicious Hard drive activity

Another warning sign of a potential malware infection on your system is the **hard drive activity**. If you notice that your disk continues to have **excessive activity** even when you don't use it anymore and there is no present program or download running at that moment, this could be the moment to check your system for malware.

I have to mention that another possible cause for the abnormal hard disk activity could be a hardware failure of the disk. This should also be taken into consideration.

5. Running out of hard drive space

Regarding the hard drive, you also need to check if your physical storage space has been increasing lately or if some of your files disappeared or changed their names. This is another sign of malware activity, since there are numerous types of malicious software which use various methods to fill up all the available space in the hard drive.

6. Unusual high network activity

There are cases where you may not be connected to the Internet with your browser and there is no program that may connect to online servers to download or upload any data, but a high network activity can still be observed.

First of all, you need to check the following:

- *Is there any Windows update at that moment?*
- *Is there any program or application that may be downloading or uploading any data?*
- *Is there any update for a certain program running at that moment?*
- *Is there a large download that you started and forgot about it and is still running in the background?*
  If the answer to all these questions is **No**, then maybe you should **check where all that traffic is going.**
- **To monitor your network,** you can use one of the following programs: **GlassWire, Little Snitch** or **Wireshark.**
- **To check for a malware infection,** use a good antivirus product to check your system.
- If you suspect that your computer has been infected by a **dangerous financial malware**, you need a specialized software designed to address these type of threats.

7. New Browser home page, new toolbars and/or your browser opens unwanted websites

Did you notice your home page has been changed and you don't seem to know why?
A new toolbar seems to be placed at top of your web browser?
Have you tried to access your favorite blog, but you were sent to a different address?

This usually happens when you visit a website and you accidentally click an online link or a pop-up window. This action triggers the download and install of a secondary software, which is not only annoying, but also malicious.

What to do:

Run a complete scan with your security solution as soon as possible. Because these type of threats don't easily go away, make sure you run additional scans with specialized software, such as anti-spyware programs mentioned above.

8. Unusual messages or programs starting automatically

If, all of a sudden, you see programs opening and closing **automatically,** your Windows operating system shutting down **without reason** or you have **strange windows** in the booting process and Windows lets you know that you lost access to some of your drives, **this is something you should worry about.**

Though it may be a technical issue, it is also a sign that **malware** could be present on the system. If this is the case and you lost access to some important areas of your operating system, you need to prepare for the worst. These are the cases when a complete wipe and reinstall of the operating system is taken into consideration.

9. Your security solution is disabled

Your antivirus solution doesn't seem to work anymore or the Update module seems to be disabled. You should know that some malware programs are specially designed to disable security programs, leaving you without any defense.

If you already tried to reboot your computer, close and open the security solution and all other normal troubleshooting steps resulted in no positive outcome, you may consider that your computer has been affected by malware.

Though you may have prepared for the worst, complemented your online security by employing advanced anti-spyware solutions and security programs specially designed to keep money safe, there are cases when a powerful malware gets beyond our defenses and compromises our security solution.

10. Your friends say they receive strange messages or emails from you

Are your friends telling you that they received suspicious emails from you or instant messages from your social media account containing attachments or links?

First of all, you need to verify whether those emails or messages were sent from one of your accounts (so **check your Sent Items** folder in your email account) or if those messages were delivered from an application which is out of your control.

If you discover the messages were sent from one of your accounts, make sure of the following:

- **Make sure you logged out from all your accounts.** *How many times didn't you access the same accounts on work computers, home laptops and even mobile devices?* Since you logged in to your favorite online accounts on so many mobile devices, it is quite possible that sometimes you forgot to log out. Therefore, always make sure to log out from your online accounts on all the devices.

- **Set strong passwords for your accounts.** Don't forget to combine upper and lowercase letters, numbers, and symbols. Don't use the same password for all your accounts. Even if you are hacked, having different passwords for each account will help you limit a potential loss. Make a habit of changing your main passwords every 30 days. Use a strong and secure password manager as LastPass.

- **Use two-factor authentication.** Use this method to make sure your online accounts or your email address are not accessed by somebody else. Using this option means that, besides entering your credentials, you will also need to enter a code sent to your phone.

Remember this: knowledge is your best weapon.

Knowing how malicious software behaves on a regular system may just prove to be the **key element** between staying **safe** and having your system wrecked or your online identity stolen.

Since we live in a threat environment, online security means not only to install a series of security programs, but **understand how malware manifests itself on the**

system and thus to know your enemy.

In the end, don’t forget that it is far easier to prevent a threat from becoming reality than to take actions against it when it’s already too late.

Lesson 17 /19

What your kids & parents need to learn about cyber security

Lesson 17

Hi there,

Today I want to help you protect some of the most important people in your life: **your children and your parents.**

Kids and parents are some of the most vulnerable categories of online users for **one simple reason**: none of them have the ability to understand what might harm them online.

Their innocence about all things web makes us smile most of times, but it could get **them** into trouble!

So let ME help YOU help THEM!

Teach your parents about online safety

Teach your kids how to use the web safely

Lesson 17

5 Tips to Protect Your Parents from Cyber Attacks

1. Explain what information security is, in their own language

You're almost at the end of the course, so you're well equipped to pass on the information you've learnt to others who might need it.

Make sure you help your parents understand the basic notions of online security, before they go online.

Knowing how to download an attachment received in an email is as important as knowing not to open an email sent by a strange person.

When talking to your parents about cyber security:

- **Do your best to use examples and comparisons** to real life events to help them understand the impact of their actions online.
- Explain to your parents that **their digital assets** (bank account, personal information, etc.) **need as much protection as their physical ones** (house, car, wallet, etc.), except that, for the most part, they can't insure their digi-

tal belongings, so they should be extra careful with how they handle the information.

- Ask them to **be careful while they shop online** and not to be deceived by the notorious **„you're our 1000000 customer!"** banner scam and the like.

2. Show them how they could get compromised

I think you've experienced this as well with other things you've read:

Examples are a great way to help information stick.

- Take your parents through some examples of how they could get infected online:
- Show them how clicking a malicious ad could infect their laptop;
- Teach them about spam and how to organize their inbox;
- Advise them not to download anything suspicious;
- Warn them against installing new software on their computer without consulting you first. For this last part I also recommend installing **Team Viewer**. It will come in handy

if something goes awry and you need to see what the situation is, so you can fix it.

A simple example is to tell them about ransomware:

Advise them to **read this story** about how someone's mother became a victim of cyber criminals and paid over $500 to rescue her data after her computer was infected with **CryptoWall**.

That's something they should remember!

3. Teach them to be vigilant

Be open and approachable about your parents' questions and never talk to them in a condescending manner.

It's important for them to **be vigilant online** and to know how to react to different triggers that cyber-criminals might use (banners, links, spam, etc.).

Of course, remember to advise them against giving their personal information for any forms or contents they may come across online.

You don't want to worry them too much, but enough to be observant, while still enjoying Wikipedia, Facebook or other websites.

4. Indicate how simple safety features work

A good way to teach your parents about security features on their laptop is to show them how to store their passwords in a safe place and to set up a password for their computer.

When it comes to paying bills, show them what **security symbols** they should be looking for (SSL, the padlock symbol, etc.) when making a financial transaction.

Teach them **what alerts to look** for when if the antivirus kicks in (you should install this right after the initial setup) or for signs of malware infection.

Also, assure them that they can give you a call anytime they have questions.

5. Install a silent patching tool

How many times have you received this call from your mom?

“Honey, there’s this box asking me to download an update or something. And I don’t know how to close it. What do I do?”

From my experience, **there's only one way to prevent this type of calls from happening** (I can't say the same about other questions though :))!

You need a tool that can patch the software on your parents' computer silently, without asking for permission or filling the desktop with popups on start. Heimdal Free can be an option you can consider.

Remember that antivirus is not enough to protect them from sophisticated threats (go back to **lesson 6** for more details on next-generation anti-hacking tools).

Now let's see how your juniors should learn, early on, how to stay safe online. This, in turn, will help them become responsible Internet users.

Internet Safety for Kids in 7 steps

1. **Establish ground rules that define Internet access and usage for your child**

   One of the most important talks you should have with your child is about **dos and don'ts while browsing the web.**

Establish the limits that define how your kids can access the web with care and patience.

Here are some of the subjects you may want to include in the discussion:

- **Personal information** – what's okay to share and what isn't
- **Screen name** – how to choose one
- **Passwords** – how to create and manage them (remember lesson nr. 4?)
- **Photos** – you kids should never post pictures online without your approval
- **Online friends** – remind them that not everything they read online is true and teach them to ask for advice before befriending someone unknown online
- **Online ads** - avoid clicking them and never buy anything online without the parents' permission
- **Downloading** – it's best to teach them to ask you before downloading a new program/app/email attachment
- **Bullying** – never respond to mean or insulting messages and always ask for help from adults
- **Social networking** – mind the age restrictions for social networking sites and help your kids perceive them not as limits, but rather as a layer of protection
- **Research** – make a list of trusted resources your kids can use and always be available for questions when they ask

for help.

As part of these limits, negotiate how often it would be okay to **check what's happening on your kids' gadgets.** It doesn't have to be daily, but once every few weeks, you should take a look at:

- Your kids' browsing history
- Their download history
- The IM applications they use
- Their email inbox
- Other communication tools and platforms they might use (chatrooms, forums, etc.).

This type of monitoring is only suitable for certain ages, **so that's why it's essential to start educating your children on cyber security at a young age.** As they grow older, they will most likely reject all forms of monitoring, especially during their teens.

Also, keep in mind that the limits we, as adults, impose may increase our kids' safety online, but at the same time we risk blocking the natural development process that drives our children forward.

Balance is key, as with many aspects regarding using the web and its many resources.

2. Teach your children about online dangers

I can't emphasize this enough:

Teaching your kids about the threats looming around the web is crucial to help them enjoy the web safely and keep your family protected.

Talk to your child/children and get them to sign off on a **mutual agreement** that teaches them how to behave responsibly on the web. Here's an example you can use:

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number without my parents' permission.

2. I will tell my parents immediately if I come across something that makes me feel uncomfortable.

3. I will not agree to get together with someone I "meet" online without first talking to my parents and asking for permission. If my parents agree to the meeting, I will make sure that it's in a public place and bring a parent along.

4. I will always check with my parents about posting pictures of myself or others online and I commit not to post any pictures that my parents consider to be inappropriate.

5. I will not respond to any messages that are mean, offending or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do, I will tell my parents straight away.

6. I will be responsible about the rules set about how and when I use the computer and phone. Along with my parents, we'll decide upon the time of day that I can be online, how long I can stay online and appropriate areas for me to visit. I will not break these rules without their permission.

7. I will not give out any of my passwords to anyone (even my best friends) other than my parents.

8. I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or mobile device, or put my family's privacy at risk.

9. I will be a responsible Internet user and never do anything that hurts other people or is against the law.

10. I will help my parents understand things they don't know yet about the Internet and other technology, while having fun together and making it a great experience.

3. Install a good antivirus product on the computer

Are your children using a separate computer from you? Are you using the same computer?

It doesn't really matter. Security is security and **each computer should be protected from online threats and malicious software.**

Since children are naturally attracted by new things and have less experience, they easily follow dangerous links and untrusted websites. Not to mention the tendency to download and install video games from unknown web locations, a content which could easily infect the entire operating system.

Therefore, **you need to have a good antivirus product from a reliable company** and this solution must include:

- ✓ a real-time scanning engine,
- ✓ a firewall
- ✓ and automatic updates for crucial software.

To help you determine what the best AV solution for you and your family is, I recommend using the guide we shared during **lesson 5** of this course.

You'll find everything you need to help you make a wise decision in there.

4. Use parental control software to monitor your child's online behavior

Software companies have already considered the possible issues that could appear from kids' unrestricted access to online content. For this reason, you'll find many parental control solutions that address and try to limit this problem.

Should you use such a software or not?
How much do you trust your child's intuition?
And how likely is it that your child will get involved in unsafe activities that could compromise the operating system or your financial situation?

Since parental control solutions have been in use for quite some years now, you may find useful having a software that acts like **an online guardian.**

Parent control solutions can help by:

- ✓ monitoring Internet usage
- ✓ keeping track of visited websites
- ✓ controlling the Internet connection time

- ✓ blocking malicious or porn websites
- ✓ blocking games
- ✓ reporting any unusual online activities.

Here are **some free options worth evaluating:**

- Romaco Timeout - **https://romacocanada.ca/timeout/**
- Parental Tools - **http://www.parentaltools.net/**
- DigiParent - **http://digiparent.weebly.com/**

+ 27 more options listed here:
http://listoffreeware.com/list-of-best-free-parental-control-software/

+ 6 more options listed here (including cell-phone monitoring apps):
http://www.tomsguide.com/us/best-parental-control-apps,review-2258.html

5. Keep your child's software up-to-date

At the risk of sounding like a broken record, I'm going to say this one more time:

Make sure the Windows operating system used by your child has all the latest security patches installed. These updates are important because they contain **stability and security fixes** that shield the system against cyber-criminals attempts.

Security experts have proved that hackers usually gain access to operating systems by using security holes in software, like Adobe Flash, Java or popular browsers like Internet Explorer, Mozilla Firefox and Google Chrome.

That's why you need to check the PC used by your children and make sure they have the necessary security patches. To avoid this task which could take some time if you have a few computers in the house, I recommend using a free dedicated solution to do the job, such as **Heimdal FREE** or **Malwarebytes Anti-Exploit kit**.

6. **Don't let them go online without anti-spyware protection.**

As you already know, **spyware** is a software program that monitors your private Internet connections without your knowledge. But, as everybody knows, there are many warning signs that could indicate that such an infection is present in your system.

So, if you hear your child complaining about **slow-down issues, pop-ups all over the screen, new toolbars, a different default engine or random error messages**, this could mean a spyware issue that you need to address.

To stay safe from spyware, talk to your child and teach him a few basic things to keep things clear:

- don’t click suspicious links or pop-up windows
- don’t answer to unexpected questions
- don’t involve in chat sessions with strangers
- be careful about drive-by downloads in free applications.

Even better, use popular anti-spyware products available online, like Malwarebytes or Spybot Search and Destroy.

7. Secure your Home Wireless network & stay safe on public Wi-fi hotspots

The home Wi-Fi network is usually accessed only by members of the same household, but that doesn’t mean that it’s danger free. You should still work on keeping things secure.

In **lesson 11**, we shared 2 essential guides for any Internet user:

How to protect your Wi-fi connection at home &
How to keep safe on public Wi-fi hotspots.

Make sure to go back on that lesson for step-by-step tips & tricks and APPLY them.

The key to cyber security is ACTION, not just information! It’s important to protect the home network and the computers that are part of it, because a security breach on one computer could compromise the entire network. And this is something you, as a parent, should be aware of.

So here’s a **final checklist** you can use that summarizes this comprehensive lesson:

Tips to Protect Your Parents from Cyber Attacks

- ✓ Explain what information security is, in their own language
- ✓ Show them how they could get compromised
- ✓ Teach them to be vigilant
- ✓ Indicate how simple safety features work
- ✓ Install a silent patching tool

Internet Safety for Kids

- ✓ Establish ground rules that define Internet access and usage for your child
- ✓ Teach your children about online dangers.
- ✓ Install a good antivirus product on the computer.
- ✓ Use parental control software to monitor your child’s online behavior.
- ✓ Keep your child’s software up-to-date.
- ✓ Don’t let them go online without anti-spyware protection.
- ✓ Secure your Home Wireless network.

That’s it for today. You’re almost at the end of the course, so kudos for sticking with us so far!

Lesson 18 /19

No-nonsense cyber security: 10 things you never knew were necessary

Lesson 18

Let’s start with a simple question:

What is common sense and how do you define it?

And the most important question is:

How can you use common sense to keep you safe online from advanced pieces of malware and cybercriminal masterminds?

Though security tools are not to be left aside, without deeper knowledge and understanding of Internet security, *going online is like driving a car without a license.*

Common sense is vital! So here are the **10 common sense guidelines** you need to be aware of before going online.

1. Copyright is important

The World Wide Web contains various types of content, like music, images, text and so on, that may fall under copyright rules.

Since the Internet content is easy to access, we have the impression of a total online freedom. Nevertheless, there are rules and laws that do not allow using someone’s content without permission.

Have you used a text or an image in a certain context? Make sure you give credits to the owner. Usually, as long as you admit and indicate the original owner and location, there should be no problem in using a specific piece of content.

2. **Be careful when dealing with emails from unknown sources**

   Have you received an email from an unknown source? Do you frequently receive emails from people you don't know?

   First, don't trust emails that come from people you never met, especially those emails that ask you to take an action.

   It is not very difficult to spot this type of phishing emails which demand immediate action and contain words like **"confirm now"**, **"take action now"**, **"discover now"**, **"pay now"**, etc.

   To fool the potential victims, the latest trend in e-crime is to deploy spear phishing attacks, where emails appear to come from well-known individuals or banking authority.

   How do they find out about your friends or companies you're usually dealing with? They simply launch an identity theft operation to target and steal your sensitive information.

So, when you receive such an email, make sure you:

- don't reply to the email
- don't click the (malicious) attachment
- don't click the dangerous links in the email that could download malware on the system

3. Don't click that link or online ad!

It is a link and you want to follow it, no matter it is in an email or in a web page.

What could go wrong? The answer is simple: **a lot of things could go wrong.**

Just by clicking a link in an email or a pop-up window, you could connect and enroll your system into a botnet network and have your computer used in online attacks and malicious actions that target financial data and personal information.

You may think that you are safe from all these dangers because you are using a good antivirus product, but today **traditional antivirus protection is not enough anymore** and you need additional weapons in the fight against online dangers.

4. It's a free program, so that's good, *right?*

Well, it depends on the program. ***Do you know that program? Have you or others used it before?*** **If you are not sure about a software that you want to download and run on your system, just google it!**

You should find some information on that software or, in case it is a malicious software, you should discover users that complain or security programs that have been created to remove that threat.

Another major danger posed by free programs is the additional drive-by downloads that are installed without our knowledge and bring on the system security exploits that target our software vulnerabilities.

Make sure you use a program that automatically updates your vulnerable software applications.

5. Do not reveal sensitive information online

It is not easy, especially today when everybody has a social media account and it's normal to simply go online and comment, blog or share.

And among so much information we make public, we forget that personal names, contact details or private interests are also displayed to unknown people.

As I have already mentioned above, these are the elements that are used to deploy identity theft activities. So, be a bit skeptical about people you meet online and about their intentions. It is a well-known fact we all exaggerate our real lives on Facebook, but sometimes social media dangers may create real issues for us if we add the wrong people to our circle of friends.

6. Keep your credentials for yourself

Our credentials for online accounts, user names and passwords, are probably the most important pieces of information in the online environment.
For this reason, there is nothing more important than keeping them safe from prying eyes and cybercriminals.

Remember: Even though you may have set a strong password, if you use it more than once and in more than one online account, in the unfortunate case hackers discover it, your other online accounts are in danger.

7. Report illegal activities or offending content

If you notice offending language attacks, like cyber-bullying, hate speech or any form of harassment, do not hesitate to report it immediately to your parents, teachers or, if you are an adult, to the law enforcement officials.

It is much better to take action sooner than later, because it all starts from a simple verbal attack that may develop into something much bigger, especially for a child.

Though it may not happen to you, it doesn't mean that a friend or a family member won't be affected by what you choose to ignore.

8. What you post online stays online forever

We post photos, remarks, location updates and similar content, which we think it is only seen by our close friends.

But, from your 200 or 300 friends, how many of them do you actually know?

And you may think that your posts and comments are usually ignored or don't receive much attention, but they still remain there and you never know when they come back at you. Not to mention the fact that search engines save and classify your content on so many online servers.

To keep it short, follow a few simple guidelines:

- think twice before you publish or post it.
- *will you still support your content over the years?*
- *could your content affect your personal or professional life in the future?*

Stay social, but stay safe. *Do you remember lesson 12, where we talked about social media protection?*

9. Use antivirus protection before you go online

Don't go online until you have the best antivirus protection that money can buy.
You may think that avoiding adult websites and that sort of thing will keep you safe, but did you know that hackers now hide malicious code even in legitimate websites?

And it's getting worse! Even if you have a good antivirus product, you may still get infected by advanced malware. And in this case, you really need the best tools out there.

To find the best antivirus product, take a fast look at lesson 4!

10. Create back-up copies for your important stuff

Though you may have all the security protection in the world, disaster may still hit your system and your valuable files.

It may be a system crash, a hard disk failure, a ransomware attack that encrypts your entire operating system or it may be a human mistake.

There are so many reasons something may go wrong for you and your sensitive information, even if you followed all the common sense in the world.

So, save your data and don't forget about the back-up solutions in lesson 7!

There is a strong connection between common sense and knowledge.

If you need to follow a set of security guidelines to stay safe on the Internet, the same thing is valid for common sense behavior in the online sphere. In the end, knowledge and common sense become the two sides of the same coin: **Internet protection.**

Lesson 19 /19

Cyber Security Ninja level achieved!

Lesson 19

You know what makes you a rockstar?

The fact that you've stuck with us for 18 lessons and now you're down to the last one!

You've gone from being a curious user to becoming **a real CYBER NINJA** in terms of information security knowledge and that is FANTASTIC! Both for you and for the ones that will benefit from your protection and insights.

I hope that one of the main things you leave this course with is this:

The ability to navigate any web environment safely.

Knowledge may evolve and cyber threats will definitely do so, but after "graduating" this course I know you will be able to spot vulnerabilities, threats and malicious intentions and shield yourself from them.

So now **it's time to see how far you've come.**

Remember the self-evaluation you did in the first lesson of the course?

We have another one prepared to show you how well you can now protect yourself and others from cyber threats. (*If you never got around to filling the first evaluation, no worries – just go ahead with this one and enjoy the results!*)

Lesson 19

How strong of a Cyber Ninja are you?

TEST YOUR CYBER KNOWLEDGE NOW

Before you say goodbye, I want to give you that surprise I promised in the beginning of this final lesson.

We put together a FREE EBOOK for you with **50+ security tips & tricks from top experts in the industry!**

And last, but not least,

as a **BIG THANK YOU for choosing this course** and investing your time and effort to enhancing your cyber security skills,

It's been a great learning experience for us as well putting together this course for you!

I hope you'll meet us on the **Heimdal Security blog**, where we'll keep building cyber security guides that can really help you every time you go online.

And here's one more reason to keep improving your Internet security: we just launched **The Daily Security Tip**! It's a daily email with quick online safety tips you can apply

Lesson 19

right away. I figured you didn't want to miss this one.

Here what it's all about:

- The Daily Security Tip is **a way to further improve your cyber security**, through easy and actionable tips;
- If you subscribe, we'll send you **an email every day** with a security tip;
- We prepared **365 tips**, enough to cover your protection for a year;
- The tips are accompanied by **a GIF guaranteed to make things fun(nier)**;
- And yes, **it's all free!**

Sign up to get your first tip

I can't wait to see what you think about it!

And if you ever want to let me know what you loved the most about **Cyber Security for Beginners** or about **The Daily Security Tip**, feel free to hit reply on this (or any other) email I send you.

Stay safe!
The Heimdal Security team

About Heimdal Security

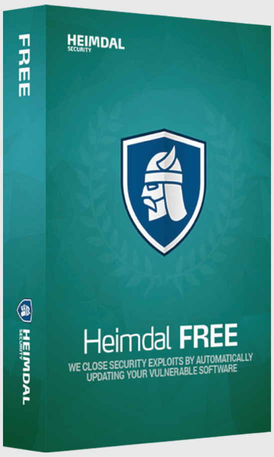
HEIMDAL
SECURITY

We are Heimdal and security is our passion

Since 2011, we have been developing new technologies and providing intelligence to protect over 350,000 users against cyber criminal attacks and data security breaches.

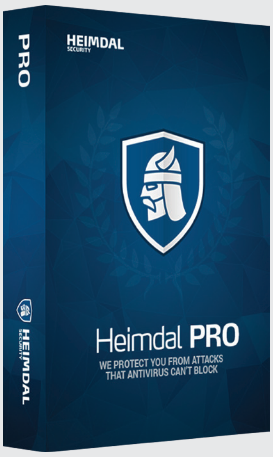
We protect users and companies from cyber-criminal actions, by keeping confidential information and intellectual property safe.

The last years proved that information theft and financial data leakage are major international issues, which continue to create security challenges for organizations, as well as private individuals. That's why our products have been developed: to address the real-world need for a solution against cyber-criminals actions and their malicious tools.


FREE
HEIMDAL SECURITY
Heimdal FREE
WE CLOSE SECURITY EXPLOITS BY AUTOMATICALLY UPDATING YOUR VULNERABLE SOFTWARE
HEIMDAL

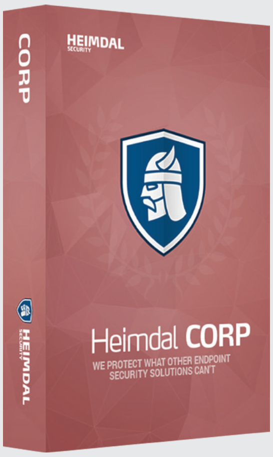
Heimdal FREE

We keep you safe from security exploits by automatically and silently updating your vulnerable software applications.



HEIMDAL PRO

We protect you from attacks that antivirus can't block, such as ransomware or sophisticated financial malware. Ensure your system is proactively protected against cyber attacks using Heimdal PRO's intelligence.



HEIMDAL CORP

We help you manage your network security from a single, easy-to-use interface to keep cyber-criminals and data stealing malware away from your company's sensitive data.