



Co-funded by the
Erasmus+ Programme
of the European Union



Content Unit

[Hardware and Software Protection]

Project: B-SAFE

Number: 2018-1CZ01-KA204-048148

Name of author: EDIT VALUE®

Last processing date: 02.09.2020



Hardware and software protection

First introduction

Hardware and software are interconnected: without software the hardware of a computer would have no function.

Digitalisation is transforming our economies worldwide. Whether at work or in private life, there are always some issues regarding hardware and software that affects all of us. In addition, hardware and software must be updated, upgraded or replaced regularly due to the existence of serious risks to organizations and also to the overall society.

In this content unit you will learn about the most common attacks concerning hardware and software and what you can do to protect yourself from that.

Do you know that most problems are software problems? For instance, computer software can fail for multiple reasons because virus and/or malware infections on your computer are very common because people often download or click in something that aims to do some damage to your computer. There are many ways to rectify software problems such as uninstalling and reinstalling, upgrading, using updated anti-virus software and checking the manufactures website for patches. But there is more that you can do as you will see in this content unit.



Practical relevance – This is what you will need the knowledge and skills for

After working through this content unit, you will know the most common types of attacks on hardware and software and also what you can do to in terms of tips and recommendations that you can apply regularly to have a better and safer hardware and software protection.

Overview of learning objectives and competences

In LO_Hardware and software protection_O1 you will know the definition of hardware and software, the main differences between these two terms and the purpose of hardware and software.

In LO_Hardware and software protection_O2 you will learn the most common attacks to software and what you can do to improve software consequences of hardware most common attacks and what you can do to improve hardware protection through some measures/tips to improve hardware safety.

In LO_Hardware and software protection_O3 you will be familiarized with the main common attacks to software and what you can do to improve software protection through some measures/tips to improve hardware safety.



Learning objectives	Fine objectives
LO_Hardware and software protection_O1: You know what hardware and software are and the most common attacks.	FO_Hardware and software protection_O1_O1: You can give the definition for the terms hardware and software. FO_Hardware and software protection_O1_O2: You can explain the purpose of hardware and software protection.
LO_Hardware and software protection_O2: You know what you can do for better hardware protection.	FO_Hardware and software protection_O2_O1: You can explain what hardware protection is. FO_Hardware and software protection_O2_O2: You can explain the main consequences of the most common attacks on hardware. FO_Hardware and software protection_O2_O3: You can give some recommendations to prevent the most common attacks through strategies regarding hardware protection.
LO_Hardware and software protection_O3: You know what you can do for better software protection.	FO_Hardware and software protection_O3_O1: You can explain what software protection is. FO_Hardware and software protection_O3_O2: You can explain the main consequences of the most common attacks on software. FO_Hardware and software protection_O3_O3: You are familiar with recommendations to prevent the most common attacks through strategies regarding software protection.

1. Build knowledge - Hardware and software and the most common attacks

Digitalisation is transforming our economies globally. Although the amount of benefits that arise with this phenomenon, there are also **advancing threats for digital security that affects safety and privacy** in our homes, cars, businesses or even networks. This is because we are constantly using digital devices in everyday life, a trend that is increasing steadily.

Therefore, the hardware and software of these devices must be **updated, upgraded or replaced** frequently due to the existence of serious risks and threats to the overall society.

But let's start from scratch: What exactly do we refer to when we talk about hardware and software? In the table below you can see a detailed definition about hardware and software.

Definition
<p>Hardware is any physical component used in or with your device, whereas software is what you have inside of your computer's hard drive, smartphone and/or tablet. Hardware is the part of your computer or smartphone, whereas software collects and processes data on your computer's hard drive. Some examples of hardware components are: computer processor (CPU), hard drive, main board, computer monitor, printer or a mouse.</p> <p>Software is the logical part of your computer or smartphone; it cannot be touched as it is immaterial. Still, all software's use at least one hardware component to operate. You can imagine software as a set of instructions that tells a device exactly what to do. It can be programmes or</p>



data. For example, a video game and Microsoft Outlook.

To make it clearer for you, you will now see the main differences between hardware and software in the following table:

	Hardware	Software
Function	<p>Hardware is a physical part of a physical device that is responsible for processing data/information</p> <p>Hardware can't function without any software</p>	<p>Software is a set of instructions that tells a computer exactly what to do</p> <p>Software is responsible to make the hardware work</p>
Characteristics	<p>Hardware are physical electronic devices that we can see and touch</p> <p>Hardware can't be affected by computer viruses</p>	<p>We can see and also use the software but can't touch it</p> <p>Software is affected by computer viruses</p>
Life cycle	They can become physically damaged	They can become outdated
Initialization	They work as soon as the software is installed	They need to be installed in the hardware to work
Maintenance	Pieces can be transferred from one place to another	They can be re-installed and transferred
Examples	Mouse, CPU, monitor, printer, hard disk etc	Microsoft Word, Firefox, Skype, Adobe Reader, etc

As we can see in the previous table, **hardware and software are interconnected** and without software the hardware of a computer would have no function.

Hardware and software protection have become a hot topic for everyone especially nowadays. But why is that the case? In the table below you can see three main purposes of hardware and software protection.

Hardware protection	Software protection
<p>1. Computer hardware can be very fragile (for example, heat, water, improper use, physical accidents caused by people are the biggest threats to a computer's physical safety)</p>	<p>1. Regular updates to software have plenty of advantages such as preventing computer bugs, weakness in software programs or operating systems</p>



2. Hardware should be properly clean in order to protect them from excessive heat	2. Software updates helps to deal with security flaws/vulnerabilities
3. Some incidents such as a robbery, water in your hardware can cause loss/theft of data, information, damage your system and data files	3. Software helps to protect your data/ precious information from external malware sources

Therefore, hardware and software security play an important role in ensuring trust, integrity and authenticity. **Let's now get to some examples that make clear why the protection of hardware and software is crucial!**

Example

Did you know that in 2011 Sony Pictures suffered an attack from a hackers group which released around 1 million user accounts including personal data (passwords, e-mails, home addresses, dates of birth etc) that broke the privacy policy of their service?

In 2017, the giant HBO was attacked and the hacker released the script of an episode of a very popular TV series (Game of Thrones) that hadn't been broadcasted and also gained access to financial documents, cast and crew contact list and other confidential information.

These types of incidents can be avoided if you have a strong software and hardware protection.

2. Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_01_01

Situation: What is the meaning of hardware and software?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

- Software is a part of the computer which can be touched.
- Hardware can be affected by computer viruses.
- **Software is responsible to make the hardware work.**
- **Hardware and software only work if they are together.**



Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_01_02

Situation: Concerning hardware and software protection please select the right sentences.

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

- The most common attacks to hardware are mainly caused by external sources.
- **Software protection must be done regularly.**
- **Software attacks are the most common therefore you should look for multiple software protections.**
- Software must be protected by some anti virus.

2. Building Knowledge - Better hardware protection

Now that you know what hardware and software is and why you should protect it, in the next two chapters you will get to know typical attacks on hardware and software and measures to avoid both.

In the next following pages, you will be in touch with the most common attacks for hardware and in order to help you protect yourself, we will give you some tips and recommendations to prevent yourself from hardware troubles.

But, first of all, you need to know what hardware protection is and what the most common attacks on hardware are.

Hardware protection is related to the **protection of the physical devices** that must be carried out by a person.

But what are the most common attacks to hardware?


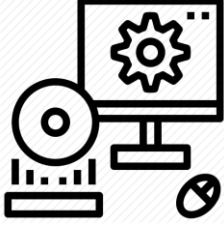
There are three attacks that happen more frequently. The two more common problems are in the table below:

HARDWARE	
Physical accidents	Modding
Physical accidents such as dropping water in a physical component or improper use can be caused by people. This type of hardware problems can compromise threats to computer physical safety	Modifying hardware, software or anything else to perform a function that was not originally conceived or intended by the original designer/future owner of the hardware

For example, the **main consequences of common attacks to hardware** are:

Modding	Malicious hardware modifications from insiders represent a serious threat. Therefore, is important to know the original source where you buy hardware components. For example, critical
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	infrastructure components like microprocessors can be inside of your computer to control you.
<p>Physical accidents</p> 	Hardware can be very fragile and also, very valuable. Heat, humidity, vibration, temperature extremes, dust, water and physical accidents to physical components are actually the biggest threats to a computer's physical safety. Therefore, you must keep all of your hardware properly cleaned, far from excessive heat sources and you should keep liquids far from the computers, smartphones and tablets.

After knowing what can happen to your hardware you must be curious about what tips and recommendations you can use to keep your hardware safe.

Please find a **few steps** to protect your hardware in the following list:

1. **Hardware modifications are illegal** unless you agree with that type of alterations. For instance, if you want you can do some modifications in your computer in order to improve something (speed, capacity, etc). Because of that, you must **avoid buying hardware components from risky sources/countries** like online platforms that are still unknown from the general public even if the price is very low and attractive because, usually, hardware that comes from untrusty sources can pose a security threat;
2. There are also **special tracking systems** that can be used to find if, for example, your hardware is stolen or lost;
3. In order to take good care to your hardware you should always **install and use updated security software**. This tip will be more detailed after when we talked about software protection;
4. **Avoid placing your hardware on high surfaces and far from heat sources, water, electrical circuit;**
5. **Clean your hardware very gently** with a dry cloth or a special tool, like long handle brush and soft bristles, wipes that you can buy on specific stores that sells hardware stuff. Keep this tip as your maintenance rule and as often as necessary.

2. Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_02_01

Situation: What is the meaning of hardware protection?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.



1. Hardware protection only depends on people.
2. Hardware protection is what a person can do to protect the physical components.
3. Hardware protection can't be done only by one person.
4. Hardware protection is only related to the implementation of physical actions/measures.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_02_02

Situation: What can happen in the case of a hardware attack?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

1. The most common attack on hardware is only related to unauthorized physical modifications.
2. Physical accidents happen more frequently because people sometimes have irresponsible behaviors/actions.
3. Attacks to hardware can compromise the personal information and the physical safety of the hardware owner.
4. Hardware attacks are related to physical incidents and modifying hardware.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_02_03

Situation: What recommendations can be implemented regarding hardware protection?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

1. Keep your hardware clean and away from heat and water sources.
2. Hardware protection should be complemented with software protection.
3. You should avoid buying hardware components from risky sources/countries due to possible unwanted alterations.
4. People can use special tracking systems and self-destructing devices if necessary.

3. Building Knowledge - Better software protection

It is now time to know more about software protection specially because there are plenty of attacks that can happen. Nowadays several software types are used by all of us and, sometimes, we won't even notice that.

Now that you know what hardware protection is you should also know the definition of software protection.

Software protection is a **computer network security architecture and methodology** that combines security devices and defensive protection from (external and internal) sources. Software protection



requires a combination of techniques related to different software. Software protection is now a critical aspect for not just companies but individuals as well.

But, what are the most common attacks to software?

Even though there are plenty of attacks to software you can find in the table below the most commons ones.

SOFTWARE			
Trojan	Malware	Virus	Phishing
Computer program that gets access to a computer or system that is camouflaged in the form of regular software in order to cause damage to system processes, hard drive data etc. Mostly introduced via e-mail attachments	Can include spyware, ransomware, viruses and worms. Malware usually happens due to dangerous clicks or email attachment that then installs risky software	Computer program that is designed to infect other computer programs, destroying essential system data and making networks inoperable	Practice of sending fraudulent communications that appear to come from a trustable source, usually through email. The goal is to steal information/data from someone (such credit card, login information, etc.)
Ransomware	Worms	Spyware	Cryptojacking
Block access to key components of your network	Malware computer program that replicates itself in order to spread to other computers	Software that enables a user to obtain information about another's computer activities	Unauthorized use of someone else's computer to mine cryptocurrency. These attacks are being done by malicious link in an email, infecting a website or online advertising

For example, the **main three consequences of common attacks to software** are:

Bugs	A common source of software security defects. Some bugs represent security vulnerabilities that may result in an information leak or unauthorized access.
Broken authentication and failure to protect data	Sometimes, functions related to authentication are incorrect and because of that some security issues can emerge. This situation can lead to unauthorized people access users' accounts to assume their identity. In this case, people can lose crucial corporate information and stolen personal information may be used to harm you and/or your clients.
Disrupt business activities	An attack to software can drive your business to




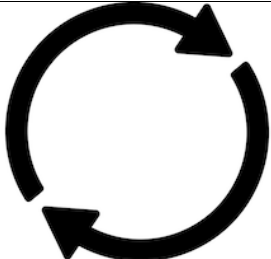
Co-funded by the
Erasmus+ Programme
of the European Union

	bankruptcy. In addition, the confidence of the customers can be affected if they know that it has been a victim of an attack.
--	-------------------------------------------------------------------------------------------------------------------------------

After seeing the most common attacks to software nowadays you need to know what you can do to prevent these types of incidents. And, after seeing some of the most common attacks you will certainly agree that protection of software is a key issue.

Please find **some hints** to what you can do to protect yourself regarding most common attacks on software:

	<p>Keep your personal information safe by using multiple strong passwords and frequent backups. You can also encrypt information.</p> <p>Create several backups of all your important data and make sure that they aren't all stored in the same place/source.</p> <p>Always keep software firewalls. To do this, you should check your hardware settings and you should have your default firewall enabled along with reputable antivirus software.</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Install updates frequently and always keep your software up to date.</p> <p>Install a phishing filter/software on your email application and also on your web browser. These filters will not keep out all phishing messages, but they will reduce the number of phishing attempts.</p> <p>Keep your operating system and security software updated.</p> <p>Run regularly scheduled scans with your anti-virus software and make sure your anti-virus and anti-spyware software are compatible.</p>
-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Never open an email attachment or run a program when you aren't 100% certain if it is a secure source.</p> <p>Verify the SSL credentials of the website and never use personal/sensitive information on websites that do not have a valid SSL certificate installed. To view the website SSL credentials please click the closed padlock in a browser window "Click the trust mark".</p>
-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	<p>Avoid using public networks.</p> <p>Deploy a website filter to block malicious websites. A website filter can help you control websites by creating an allowed list or blocked list. Please see in this website how you can do that: www.currentware.com/web-filter.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

As we can see, **prevention is the key** to avoid software problems and being proactive, in other word, take some actions to protect yourself is always the best option.

To finish, it is important to keep in mind that attacks are evolving every day and, because of that, you need to **stay up-to-date on the latest attacks and protection measures**. The main goal is to stay current with what malware is out there, it's about ensuring your security.

5. Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_03_01

Situation: What is the meaning of software protection?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

1. **Software protection combines requires a combination of multiple techniques and methods.**
2. **Software protection is mostly reactive.**
3. Hardware and software security should be a priority but software protection needs to be done more frequently.
4. **Software protection is more important because people use more software daily.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_03_02

Situation: What can happen in the case of a software attack?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.

1. **A common consequence of a software attack is the information leak.**
2. **Another common consequence of a software attack is unauthorized access.**
3. **It is very common to have financial loses in the case of a software attack.**
4. **Broken authentication and failure to protect often happen at the same time.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Hardware and software protection_03_03

Situation: What recommendations can be implemented regarding software protection?

Task: Pick the right(s) option(s) following the multiple-choice principle: None, one, more than one or all options can be true.



Co-funded by the
Erasmus+ Programme
of the European Union

1. People must implement several methods to protect the software and realize performance tests as often as possible.
2. Having updated firewalls, anti-virus, phishing filters are examples of software protection.
3. Because attacks are becoming more complex the use protection methods must be updated.
4. Because software attacks are evolving software protection measures should also be updated.

Sources

Diana, J. (n.d.). *Hardware e Software*. <https://www.todamateria.com.br/hardware-e-software/>

Hossain, F. R. (July 4 2018). *Importance of Security in Software Development*. Retrieved from <https://medium.com/brainstation23/importance-of-security-in-software-development-f92669838a90>

Images:

https://www.google.com/search?q=trust+symbol&tbm=isch&ved=2ahUKEwjBmqGzoPoAhVFEhoKHfAFDCIQ2cCegQIABAA&oq=trust+symbol&gs_l=img.3..0j0i7i30i9.3932.4753..5400...0.0..0.144.230.1j1....0....1..gswizimg.....0i10i19j0i7i30i19.OAgckFFNM7Q&ei=2xVhXoHBLcWkaPCLsJAC&bih=625&biw=1366&rlz=1C1GCEU_pt-PT#imgsrc=mN-kWUAz8wqOvM

www.shutterstock.com/search/stop+symbol

www.shutterstock.com/pt/search/update+icon

medium.com/@kluce305/rivetz-platform-cyber-security-with-blockchain-technology-1518d691cfa0

https://www.google.com/search?q=hardware+symbol&tbm=isch&ved=2ahUKEwj1orXBzoPoAhUXwIKHYd_A2lQ2cCegQIABAA&oq=hardware+symbol&gs_l=img.3..0i19l2j0i7i30i19j0i7i5i30i19j0i5i30i19l3j0i8i30i19l2j0i7i30i19.114272.115896..116061...3.0..0.123.1099.6j5.....0....1..gswizimg.....0i7i30.z7Ze f8YKloU&ei=4hVhXvWpFpeAlwSH_42QBg&bih=625&biw=1366&rlz=1C1GCEU_pt-PT#imgsrc=uvu4JDot9OTNFM

Save Knowledge

Hardware and software protection are essential aspects of security, **being responsible to preserve valuable software assets** due to **malicious activities on software**.

Although **hardware and software are interconnected**, and without software the hardware of a computer wouldn't work, and vice versa, hardware and software are two different things: **Hardware** is any **physical component** used in or with your device, whereas **software** is the **logical part** of your computer, or other device. Some examples of hardware are the main board, computer monitor, printer or a mouse, and some examples of software are a videogame or a program like Microsoft Office.

Even though it is impossible to avoid the possibility of having a hardware or software incident there are multiple measures/tools that you can follow to prevent yourself in the best way that you can. The **hardware is exposed to human error**, becoming damaged without proper care, like regular cleanups and physical protection against the elements (water, heat, *cold*, etc.). **Software** is exponentially more



Co-funded by the
Erasmus+ Programme
of the European Union

sensitive to external threats: it **can be affected by cyberattacks** such as Trojan horses, viruses, phishing attacks, spywares, malwares, between many others. Therefore, it is crucial that you take measures to minimize the risk of cyber threats. For instance, you must use **multiple strong passwords and frequent backups**, keep **software firewalls** and an **updated antivirus**, as well as deploy a **website filter** to block malicious websites.

As we can see, **prevention is the key** to avoid software problems, hence the solution is being proactive. In other word, the best option is always to take some actions to protect yourself from cybersecurity threats!

To conclude, it is important to keep in mind that attacks are constantly evolving and, because of that, you need to **stay up-to-date on the latest safety behaviors and protection measures**.