



## Content Unit [Cybersecurity]

*Project: B-SAFE*

*Number: 2018-1CZ01-KA204-048148*

*Name of author: EDIT VALUE®*

*Last processing date: 02.09.2020*

Funded by the  
Erasmus+ Programme  
of the European Union



*"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."*



# Cybersecurity

## First introduction

Have you experienced some malicious attack where, for example, someone tried to steal an important document or private information through a link present in an email? If something like that happened to you were cybersecurity victim.

Nowadays, cybersecurity is a big concern. **Cybersecurity involves preventing and detecting digital attacks, protecting systems, hardware and software.** Cybersecurity is also related to preventing, detecting, responding and recovering from cybersecurity incidents that can be intended or not. Usually, cyberattacks are aimed at **accessing, changing, theft or destroying data/information, extorting money or interrupting normal businesses** and critical infrastructures. Did you know that according to recent studies the total cost of cybercrime for each company is around 12.000.000€? Therefore, cybersecurity is a current debate that needs to incorporate society as a whole, since each person has an important role regarding the protection of their own digital information.



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

Cyberattacks are happening all the time, meaning that keeping software, hardware and data safe and secure is more important than ever. Despite this, there is only a shortage of people with these skills so learning how to get started in cybersecurity can help you with your own personal internet safety.

After learning this content unit, you will get in touch with the term cybersecurity and why cybersecurity is so important nowadays. Additionally, in this content unit you will know what you can do to take some cybersecurity measures in your everyday life.

## Overview of learning objectives and competences

In LO\_Cybersecurity measures\_01 you will learn the definition of cybersecurity and the main laws in Europe concerning this topic

In LO\_Cybersecurity measures\_02 you will know what you can do regarding password safety

In LO\_Cybersecurity measures\_03 you will know what you can do to protect yourself during online shopping

In LO\_Cybersecurity measures\_04 you will learn about cloud security

Learning objectives	Fine objectives
LO_Cybersecurity measures_01: You will learn the basic definition of cybersecurity and the main laws on this topic	FO_Cybersecurity measures_01_01: You can give the definition of cybersecurity



LO_Cybersecurity measures_O2: You will know what you can do about password safety	FO_Cybersecurity measures_O2_O1: You can explain the most common password problems FO_Cybersecurity measures_O2_O2: You can name the essential steps to have a safer password protection
LO_Cybersecurity measures_O3: You will know what you can do about online shopping	FO_Cybersecurity measures_O3_O1: You know the types of information you give regarding online shopping FO_Cybersecurity measures_O3_O2: You can explain how to improve your online shopping behavior
LO_Cybersecurity measures_O4: You will learn about cloud computing	FO_Cybersecurity measures_O4_O1: You can give the definition of the term “cloud computing” FO_Cybersecurity measures_O4_O2: You can give recommendations about what you should do when using cloud computing services/solutions

## 1. Build knowledge - Cybersecurity - definition and legislation

Data protection and cybersecurity are becoming essential values for society. Because of that, these two areas have recently undergone significant legal development and now are more consolidated in the EU. However, eliminating threats and cyber attacks is almost impossible so using cybersecurity measures and strengthened cybersecurity capabilities is mandatory.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people and hackers are becoming more innovative. In today’s connected world, everyone benefits from advanced cybersecurity measures. At an individual level, a cyberattack can result in everything from identity theft, to extortion attempts, to the loss of important data.

But what exactly do we mean by “cybersecurity”?

### Definition

**Cybersecurity** is the practice of **defending computers, servers, mobile devices, electronic systems, programs, networks and data from malicious attacks, damage or unauthorized access**. There is no standard, especially universally accepted definition of cybersecurity. In other words, cybersecurity is related to all safeguards and measures adopted to defend information systems and their use against unauthorised access, attacks and damage to ensure the confidentiality, integrity and availability of data.

## 1. Apply knowledge

### Exercise MULTIPLE CHOICE

Associated fine objective: FO\_Cybersecurity measures\_O1\_O1

*Situation:* What is the meaning of cybersecurity?





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

- Cybersecurity includes the defense of hardware and software.
- Cyber attacks are increasing and everyone is now more vulnerable to these types of incidents.
- Effective cybersecurity measures include the application of multiple cybersecurity measures.
- Cybersecurity training should be provided as early as possible due to the need of application of multiple cybersecurity actions.

## 2. Build knowledge - Cybersecurity- password safety

Do you know the easiest way for a cybercriminal to gain access to your bank, social media, email and other private data? It's a **weak password**. In fact, most of the passwords will be cracked in a "blink of an eye". According to Nacional Cyber Security Centre, the five most common passwords in 2019 were "123456", "123456789", "qwerty", "password" and "111111". So, if you have some of those passwords, or similar ones, please take a look at the example below.

Example	
Amount of Time to Crack Passwords	
 *****	
123456	0,29 ms
potato	1,37 ms
Potato	3,28 s
P0tat0	1h 23m.27s 0.10ms
P0tat0!	1 month, 3 weeks, 5 days and 21h 54min, 40s 8ms
!AtE27P0taT0s!	47623938 millenniums, 8 centuries, 73 years and 8 months

One of the most common problems with passwords is that they are generally easy to guess. Many people think that a short password with lots of different characters types is secure when, in fact, the reality is that the only way to ensure a truly secure password is to make **at least 14 characters long and somewhat arbitrary**. In addition, as you can see, **the more complex your password is, the more difficult it is to guess**. A strong password is a combination of letters (capital and lowercases), numbers and symbols. A good way to never forget your unique password is to choose a sentence instead of words, mixing it with alphanumeric characters - most websites even allow spaces between words! Nevertheless, there are more aspects to consider when creating new accounts and digital profiles to fully maximize your cyber safety and protection. Below you can observe very common "DOs" and "DON'Ts" regarding passwords. If you follow these "golden rules", your passwords are almost indecipherable to hackers.

<b>DON'T:</b> Use the same password for every account
<b>DO:</b> Create unique passwords to unique accounts and profiles

We all know that today almost every website requires an account and almost everyone uses the same passwords for different accounts. However, people often forget that these accounts contain identity or financial information about them that can be stolen or compromised and by using only one password you become an easy target for cyberattacks.



**DON'T:** Save your passwords in another source

**DO:** Memorize your passwords and setup security questions on your accounts

One easy way that is often used to remember passwords is to store them in a spreadsheet, hard drive or in personal notes. **Try to memorize your passwords!** You can also set up security questions on your accounts as a precaution. However, instead of setting common questions like “What is your mother’s name?” or “Where are you from?” use questions which only you can answer.

**DON'T:** Share passwords with others

**DO:** Be secretive with your passwords

Right after using the same password for every account another common mistake is related to the fact that people share their passwords with others by e-mail, text messages or social media. In order to keep your passwords safe, you must **change passwords with regularity**. Remember that somewhere in the world there is a hacker that keeps trying to steal user’s passwords and, the more time they have, the higher the risk of them to succeed.

**DON'T:** Choose a strong password and stick with it

**DO:** Change your passwords every three months

Most browsers and applications allow users to save their credentials so they don’t have to insert them every time they want to login. Despite being very convenient, keep in mind that if you lose your devices and a stranger manages to crack you access password, all that information is accessible to that person.

**DON'T:** Use one authentication factor

**DO:** Add two-factor authentication for every digital account

If you **use two-factor authentication** on your digital accounts, it will add an extra layer of security to them. When someone logs into your account from a new location, device or browser you will be receive a **password**, which needs to be entered for logging into your account. Apart from that, another type of two factor authentications is a **fingerprint, a voiceprint or a code sent** to your phone. Many people think this is time-consuming but if you are seriously concerned about your privacy you should use a two-factor authentication for your digital accounts when this option is possible. When you don’t have the option to use a two-factor authentication you should follow the recommendations that were mentioned before.



## 2. Apply knowledge

### Exercise SINGLE CHOICE

---

Associated fine objective: FO\_Cybersecurity measures\_02\_01

**Situation:** Please select from the following sentences the right one.

**Task:** Pick the right(s) option(s) following the multiple-choice principle: only one sentence is true.

- It is recommended to choose a simple password in order to better memorize it.
- Some unique passwords are derivative of a given name, the name of a family member or the name of a pet.
- The more characters and symbols the passwords contain, the less difficult they are to guess.
- **A strong password has a combination of uppercase and lowercase letters, symbols and numbers, and at least eight characters long.**

### Exercise MULTIPLE CHOICE

---

Associated fine objective: FO\_Cybersecurity measures\_02\_02

**Situation:** What are some of the rules to protect your digital accounts from cyberattacks?

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

- Use the same password in multiple websites/accounts.
- **Change passwords regularly.**
- Save the login credentials to a particular computer's browser or application.
- **A fingerprint, voiceprint or a pin code are good choice to a two-factor authentication.**
- **When creating a new password steer clear of words found in the dictionary, pronouns, usernames, and other predefined terms, as well as commonly used passwords.**

## 3. Build knowledge – Online shopping

As we have seen before, cybersecurity evolves the connection between people and the application of practices that aims to protect information from malicious attacks.

In 2019, e-commerce was responsible for around \$3.5 trillion in sales and is expected to hit \$4.9 trillion by 2021. In addition, 21.8% of the population worldwide shops online and brands are becoming more and more active on social media which means that they are engaging more with people through different online channels.

Nowadays, more and more people prefer online shopping over conventional shopping. Some of those advantages are related to the convenience, price comparisons, comfort and accessibility. Usually, when you buy online, you need to create an account. Consequently, you are obligated to give some of your private information, like “name”, “address”, “phone number”, “email” and a method of payment. Having this in mind, and because everything on internet is tracked, it is not a surprise that all of the data that results from the huge amount of ecommerce and interactions on social media means that it is important to know more deeply about the potential consequences of these actions.

If you want to avoid internet scams while shopping online - you'll need to take a few precautions. Below you can find a few suggestions:



### Know who you are dealing with

Read reviews and see if other consumers have had a positive or negative experience with the website. Make sure the site is security enabled.

### Monitor your financial accounts

Read your statements regularly, making sure they reflect the charges you authorized.

### Pay by credit or charge card

Credit cards are generally the safest option as they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Consider using a virtual one-time credit card. Virtual credit cards are unique credit cards that allows you to transact on your main credit card account without using or exposing your main credit card account number. For example, you can use Capital One to create this type of credit cards.



### Check out the privacy policy

Privacy policy describes how your personal information is collected, used and shared when you visit or make a purchase from an online store. You should read the privacy policy and see if you agree with the privacy of the company.

### Free can be costly

Free screen savers, e-cards or others could contain viruses. Keep your anti-virus and anti-spyware updated along with your firewall.

### Don't email your financial information

Legitimate companies don't ask for financial information via email or pop-up message.

## 3. Apply knowledge

### Exercise MULTIPLE CHOICE

Associated fine objective: FO\_Cybersecurity measures\_O3\_O1

**Situation:** What are some of the information that you should never give while online shopping?

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

- Social Security number.
- Credit card security code.
- Debit card number.
- Bank account number.
- Email address.

### Exercise MULTIPLE CHOICE

Associated fine objective: FO\_Cybersecurity measures\_O3\_O2

**Situation:** From the list, please select the right behaviors in order to avoid becoming a victim of cybercrime

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





- Before giving the credit card information, enough time must be taken to research the website.
- Buy from a website that has encryption.
- Read the website’s return policy and other terms and conditions, as well as the site’s privacy policy, before ordering anything.
- Pay by a debit card, cash or wire transfer.
- Use a “hotspot” to protect your confidentiality.

## 4. Build knowledge – Cloud Computing

Long gone are the days that you saved your files on a compact disc or even a pen drive, always with the dreadful feeling that you would eventually misplace those to never be found again. Nowadays, you can access your files on any computer and, in fact, currently cloud solutions are becoming more and more used worldwide on day-to-day activities.

You are constantly interacting with some type of cloud solutions when you are checking your email or while you are using your phone to check traffic conditions. With **cloud solutions your data is stored with a provider and accessed over the internet.**

Hence the question arising in this context is whether our data is safe and secured in the cloud? Because of that, it is important to know more about the concept of cloud computing.

### Definition

**Cloud computing** can be defined by the **delivery of on-demand IT resources** - such as storage, computing power or data-sharing capacity - over the internet, through hosting on remote servers. In other words, cloud computing means storing and accessing data and programs over the internet instead of your computer’s hard drive. These resources include tools and applications like data storage, servers, databases, networking and software. Cloud solutions are a very popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance and security.

The cloud, big data and the digitalization of industry is accompanied by a growth in the exposure of vulnerabilities, enabling malicious people to target even more victims. The variety of attack types and their growing sophistication make it genuinely difficult to keep pace. Because of that, it is important to **implement some daily precautions in order to avoid theft, leakage and/or deletion of important information.**

Please see a brief summary of some measures that you can use in order to improve cloud computing security.

<p><b>Use a multi-factor authentication</b></p>	<p>The traditional username and passwords combination is often insufficient to protect user accounts from hackers and stolen credentials is one the main ways hackers get access to your data/information.</p> <p>Because of that, you have to use not only <b>strong passwords</b> but also a <b>multi-factor authentication</b> - also known as two factor authentication - to ensure that only authorized personnel can log in your cloud apps and access that sensitive data.</p> <p>A multi-factor is one the most effective ways of keeping hackers from accessing your cloud applications. Some examples of multi-factor authentication are a password combined with a code sent over SMS or a number generated by an app.</p> <p>It is also important that you always remember to log-out and never save your credentials.</p>
---	--





<b>Manage your user access to improve cloud computing security</b>	<p>Most people don't need access to every piece of information, every application or every file. Therefore, <b>setting proper levels of authorization</b> ensures that each person can only view or manipulate the applications or data/information.</p> <p>If someone has access to everything and gets tricked by a phishing email and inadvertently provides their log in information, the hacker has access to all the information very easily.</p>
<b>Monitor, log and analyze user activities with automated solutions to detect intruders</b>	<p><b>Real-time monitoring and analysis of user activities</b> can help you notice eventual irregularities that deviate from normal behaviours/patterns. These unusual activities could indicate a breach in your system so catching them early on can stop hackers in their tracks and allow you to fix security issues before things go wrong.</p> <p>You can find many solutions for automated 24/7 networking monitoring and management and moving up to advanced cybersecurity solutions. Because every business/people has different needs for different levels of cybersecurity be sure to get a third party for risk assessment before making a big investment.</p>
<b>Anti-phishing training</b>	<p>Hackers can gain access to secure information by stealing credentials through some techniques such as phishing, spoofing websites and social media spying.</p> <p>Because of that, keep in mind that, for instance, <b>phishing training</b> should be a continuous process that needs to be managed by someone within the organization in order to make it effective.</p>
<b>Back up files in different cloud accounts</b>	<p>Regardless of scale, industry, region and/or people, ensuring data availability is a priority for everyone. In addition, losing data/information due to human error is very high so don't put all your important data in one place.</p> <p>Whether you're protecting and accessing the files on your personal laptop or you're a managed service provider responsible for a portfolio of business (and their growing amounts of data), cloud apps are essential in the modern digital world.</p> <p>Therefore, it is crucial to find <b>more than one cloud-to-cloud backup solution</b> to ensure a copy of the data you create, store and share in a safe location.</p>

## 4. Apply knowledge

### Exercise SINGLE CHOICE

Associated fine objective: FO\_Cybersecurity measures\_O4\_O1

**Situation:** Regarding cloud computing which statement is true?

**Task:** Pick the right(s) option(s) following the multiple-choice principle: only one sentence is true.

- In Platform as a Service (PaaS) a company *pay-as-they-go* for services such as storage, networking, and virtualization.
- Infrastructure as a Service (IaaS) is a cloud computing model in which a third-party provider delivers hardware and software tools Bank account number



- **Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.**
- While using cloud computers, users and companies have to manage physical servers.

## Exercise MULTIPLE CHOICE

---

Associated fine objective: FO\_Cybersecurity measures\_O4\_O2

**Situation:** From the list, please select the right behaviors in order to avoid becoming a victim of cybercrime

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

- **Store information like addresses, phone numbers, bank information, etc. in different clouds.**
- **Create a unique password solely to the cloud service.**
- While using cloud solutions it's not relevant to have an antivirus.
- Because of its convenient, it is suggested to save login credentials in the corresponding application.

## Sources

Alexandra, Susan (April 04, 2019). 10 Tips for Keeping Your Personal Data Safe on Social Media. Retrieved from <https://securitytoday.com/Articles/2019/04/04/10-Tips-for-Keeping-Your-Personal-Data-Safe-on-Social-Media.aspx?Page=2>

Cucu, Paul (December 21, 2016). 17 Underused Online Shopping Security Tips. Retrieved from <https://heimdalsecurity.com/blog/online-shopping-security-tips/>

European Commission (March 2019). Briefing Paper: Challenges to effective EU cybersecurity policy, Briefing paper. European Court of Auditors.

Federal Trade Commission (n.d.). 9 Online Shopping Tips. Retrieved from <https://www.yumpu.com/en/document/read/4010016/nine-online-shopping-tips-federal-trade-commission>

Kapiswe, Subham (April 23, 2019). NCSC Reveals List Of World's Most Hacked Passwords. Retrieved from [https://en.wikipedia.org/wiki/List\\_of\\_the\\_most\\_common\\_passwords#cite\\_note-NCSCList-15](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#cite_note-NCSCList-15)

Kaspersky (n.d.). Safer Online Shopping. Retrieved from <https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping>

National Cybersecurity Alliance (n.d.). Online Safety Basics: Online Shopping. Retrieved from <https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/>

Acronis (n.d.). Case study: The Benefits of Cloud-to-Cloud Backup Solutions from Acronis. Retrieved from <https://www.acronis.com/en-us/articles/cloud-to-cloud-backup/>

D'Silva, Frank (June 15, 2020). 6 Tips for Improving Cloud Computing Security. Retrieved from <https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security>



## Save Knowledge

The era of the internet gave us the superpower of omnipresence. It narrowed the gaps between people, businesses and places, allowing people to be anywhere and with anyone with just a *click*.

As you have learnt throughout this content unit, **online privacy and security of personal information is a shared responsibility between all parties:** government, software developers, cloud services providers, companies and end users.

With the implementation of the GDPR the end users gain confidence in their data protection as this regulation aims to safeguard people's privacy in the internet. However, there are a lot of behaviors that the end users need to adopt to play their part. Those behaviors are common to all activities in the internet – from social media to the cloud – and, are commonly referred to “the golden rules of the internet”.

The first rule relies to passwords: **have unique and strong passwords with two-factor authentication** while logging-in and **changing them every three months**.

The second rule is related to private information: **don't save or share sensible information over the internet**, especially when online shopping; moreover, if you have private information stored in a cloud service, be sure that you **don't aggregate all of your information in only one cloud!**

The third rule is practicing smart browsing: **don't save your login credentials** in any browser, website or application, and logout every time you quit a website. Equally, **don't click in any dubious link** or enter your information in unsecured websites.

Overall, you must acknowledge that it is your data that could eventually be compromised by cyberattacks and, consequently, you must assure that you comply with your part in the privacy and security of data in the internet.