



RETAIL PROJECT

ADDITIONAL CONTENTS

Cyber security in the
process of
digitalisation

RETAIL PROJECT

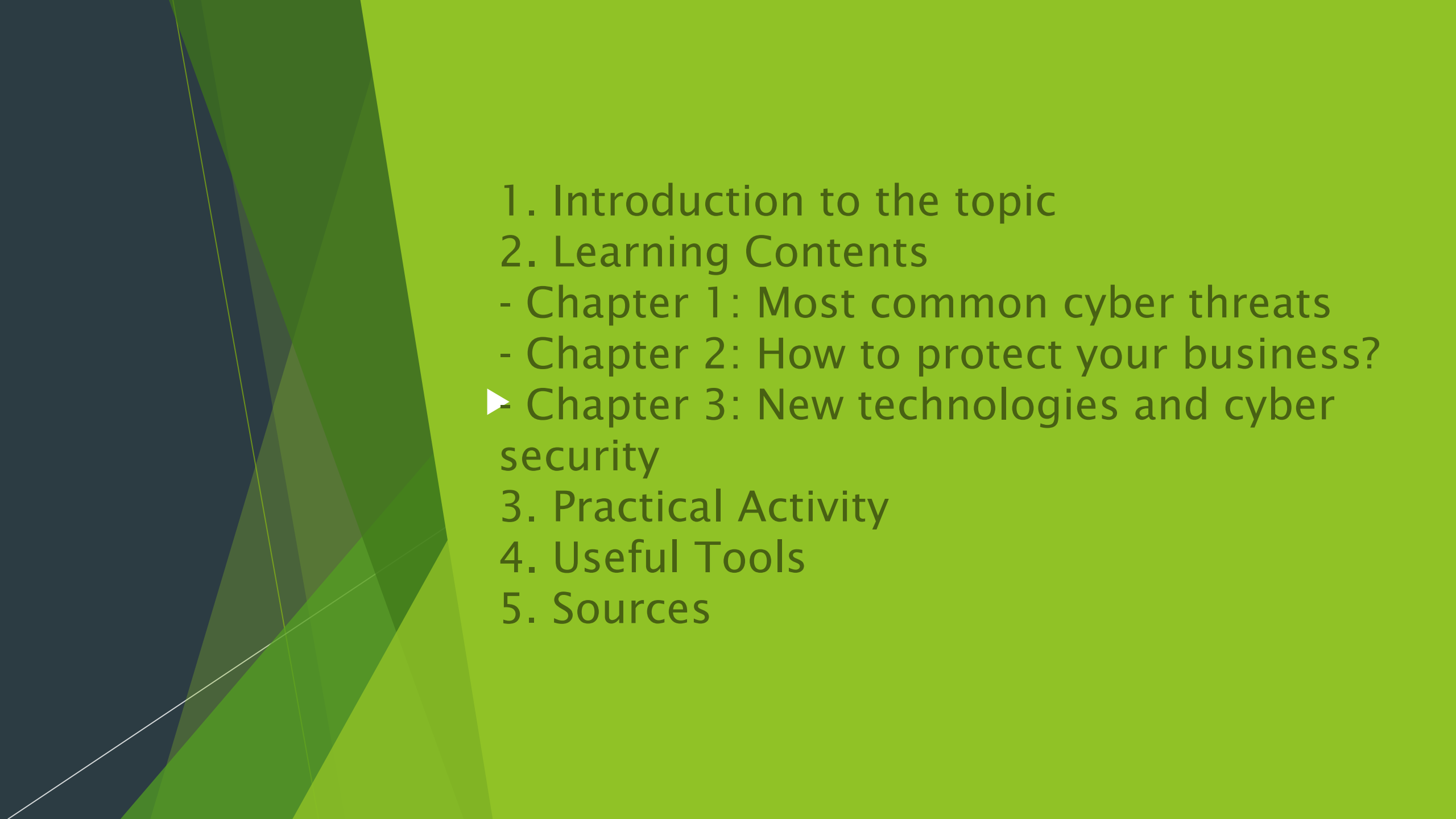


Erasmus+

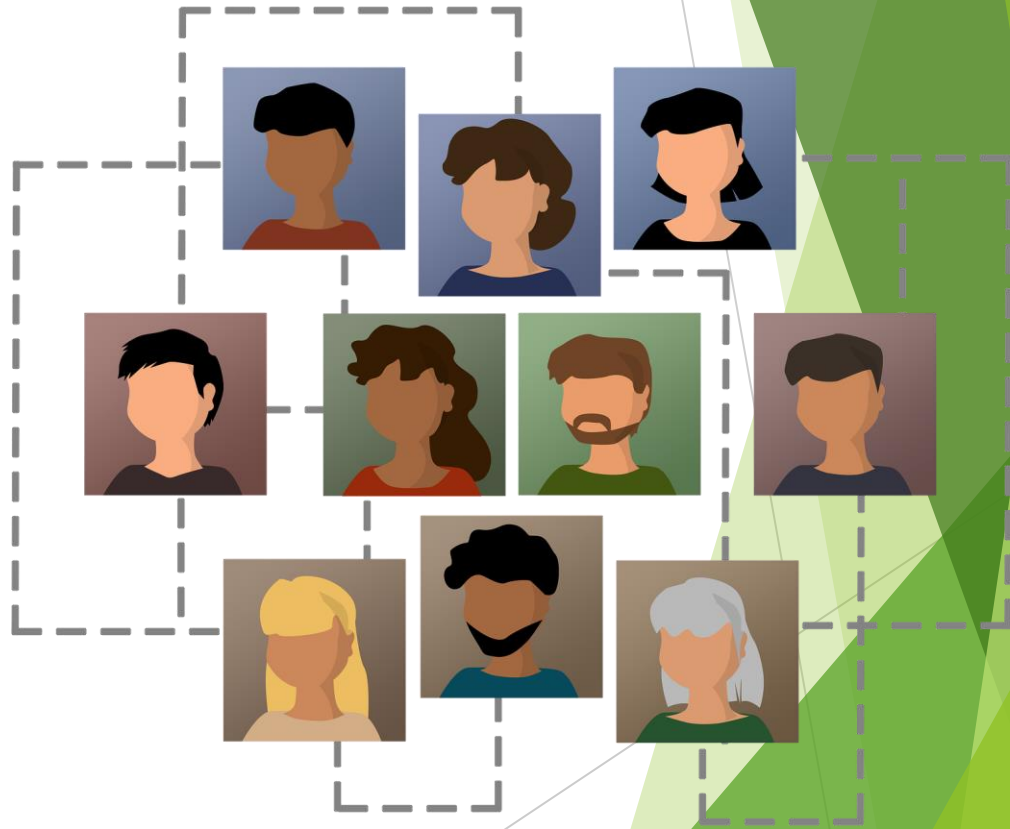
Project funded by:

**Erasmus+ / Key Action 2 -
Cooperation for innovation and the
exchange of good practices, Strategic
Partnerships for VET education**

Retail Project [www: retail.erasmus.site](http://www.retail.erasmus.site)

- 
1. Introduction to the topic
 2. Learning Contents
 - Chapter 1: Most common cyber threats
 - Chapter 2: How to protect your business?
 - ▶ Chapter 3: New technologies and cyber security
 3. Practical Activity
 4. Useful Tools
 5. Sources

1. Introduction to the topic



Covid-19 has forced many companies to accelerate their digital transition. Digitisation can support a company's operations and allow it to grow in an unprecedented manner by supporting its operations, however, it can also be a gateway to cyber attacks or data theft. Therefore, it is important to prepare for this possibility and to know how we can secure our businesses.

Each company must naturally carry out actions tailored to its profile and level of digitalisation, but there are a few common points to look out for when working to ensure cyber security.

2. Contents

This additional module will be divided into 3 chapters, a practical activity, references and further tools.

- Chapter 1: Most common cyber threats
- Chapter 2: How to protect your business?
- Chapter 3: New technologies and cyber security



2.1. Most common cyber threats



CONTENT OF CHAPTER 1
Most common cyber threats

1. Malware

Malware is short for "malicious software" and may be a code fragment / program whose purpose is to disrupt operations, steal data or damage hardware. These include popular trojans, worms and spyware.

2. Phishing

This is impersonating an individual or institution and attempting to extort money / data from the user.

3. Man-in-the-Middle

A hacker "walks in" between the interactions of 2 entities through, for example, poorly secured Wi-Fi with the intention of stealing information, personal data, etc.

2.2.1. How to protect your business?

Basically, there are two main elements you need to pay attention to

Human Resources



Statistics show that the vast majority of cyber threats are due to poor employee training and human error.

Hardware resources



This includes all computers, laptops, software, anti-virus and possible gateways used for attacks from hackers.

CONTENT OF CHAPTER 2

How to protect your business?

Human resources and cyber security

Hardware resources and cyber security

Personal data protection

2.2.2.

Human resources and cyber security

Human resources play a critical role in ensuring cyber security

It is estimated that up to 90% of cyber security problems are related to human error. Security threats can manifest in a variety of (potentially dangerous) behaviours such as: connecting external devices (like USB drives) that may be carrying dangerous malware or opening emails that come from unknown sources. There are many dangerous practices, but the most common source of the problem is gaps in employee education about cyber security.

- To counteract this in SMEs it is recommended that they:
- Create a plan of security policies, procedures, and countermeasures.
- Ensure that there are professional employee inductions in the workplace with demonstrations of the various dangerous behaviours that should be avoided.

CONTENT OF CHAPTER 2

How to protect your business?

Human resources and cyber security

Hardware resources and cyber security

Personal data protection

2.2.3.

Hardware resources and cyber security

Hardware resources must be properly secured to protect the data collected by the company

Ensuring that your equipment is properly protected against possible cyber attacks is very important. A variety of tools are available for this purpose.

The most obvious protection is to have anti-virus software. You can find a list of examples here:

<https://www.usnews.com/360-reviews/antivirus>

Firewalls are also a necessity. Although their effectiveness is not as high as it once was and a skilled hacker can bypass them, they are still the first line of defence and can prevent unauthorised entry into the system. If you decide to trade online, this of course opens up a whole new set of security challenges (especially for customers). You should start by ensuring that your shop is properly secured with SSL and TLS (the technology responsible for encryption and HTTPS - the popular padlock next to the website address).

CONTENT OF CHAPTER 2

How to protect your business?

Human resources and cyber security

Hardware resources and cyber security

Personal data protection

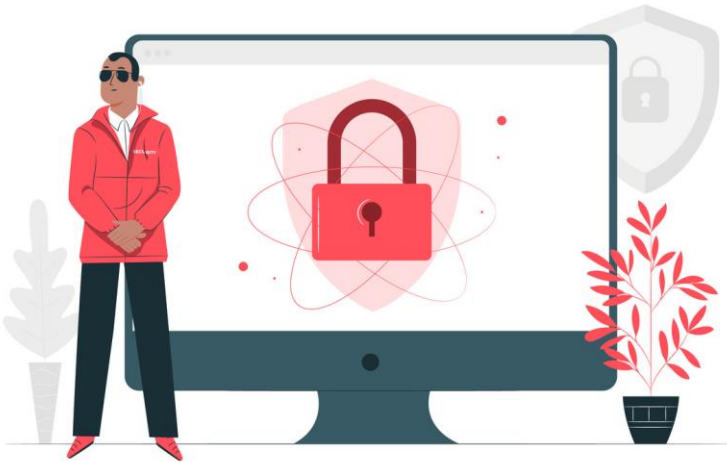
2.2.4. Personal data protection

Caring about cyber security is also about caring about the data and information you store, including the personal information of your customers and employees.

GDPR has been in force in the European Union since 2018 (whole regulation available [here](#)).

This means that data storage must comply with certain protection measures.

GDPR has introduced new rights for citizens (for example, the "right to be forgotten") and new obligations for businesses both in their physical and online operations. Among such obligations is, for example, the obligation to introduce privacy principles at the design stage (for example, of a shop). These are: privacy by design or privacy by default.



CONTENT OF CHAPTER 2

How to protect your business?

Human resources and cyber security

Hardware resources and cyber security

Personal data protection

2.3. New technologies and cyber security



CONTENT OF CHAPTER 3
New technologies and cyber security

The fourth industrial revolution (Industry 4.0) is leading businesses into a new era of connected devices. While its positives are numerous, it also brings with it certain risks. One of these is connected with the Internet of Things, which, in simple terms, involves connecting a multitude of devices that can interact without human involvement. This carries the risk that such a large number of connected devices (it is estimated that there will be as many as 25.4 billion IoT devices in 2030) will be a gateway for hackers who, by breaking into the less secure devices, will be able to access the most important elements of the infrastructure in companies.

3. Practical Activity

To practice, think about the level of cyber security in your company.



1. What training are you providing your employees?
2. How can you improved your own cyber security competencies?
3. Is your customer data well protected?
4. Are you using up-to-date anti-virus software?
5. Do you have a plan in case a cyber incident occurs?

4. Useful Tools



GDPR

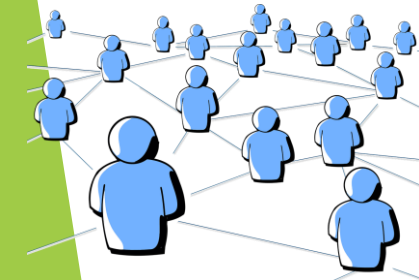
Link: <https://gdpr-info.eu/>

Video about cyber security

Link: <https://www.youtube.com/watch?v=inWWhr5tnEA>

Cybersecurity for Small Business

Link: <https://www.fcc.gov/general/cybersecurity-small-business>



5. Sources

Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks:

Link: <https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/>

Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk:

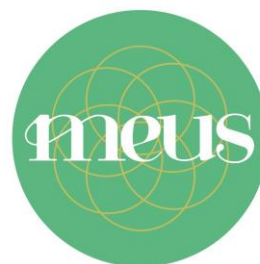
Link: <https://www.cybintsolutions.com/employee-education-reduces-risk/>

What is GDPR (Polish)

Link: <https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-rodo-i-jakie-zmiany-wprowadza-nowa-ustawa-parlamentu-europejskiego>



RETAIL PROJECT Partnership



POLISH CHAMBER OF COMMERCE

Retail Project [www: retail.erasmus.site](http://www.retail.erasmus.site)