Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Training module title:ICT Tools to prevent and recognize Cyber Risk in the Digital World

By Internet Web Solutions.

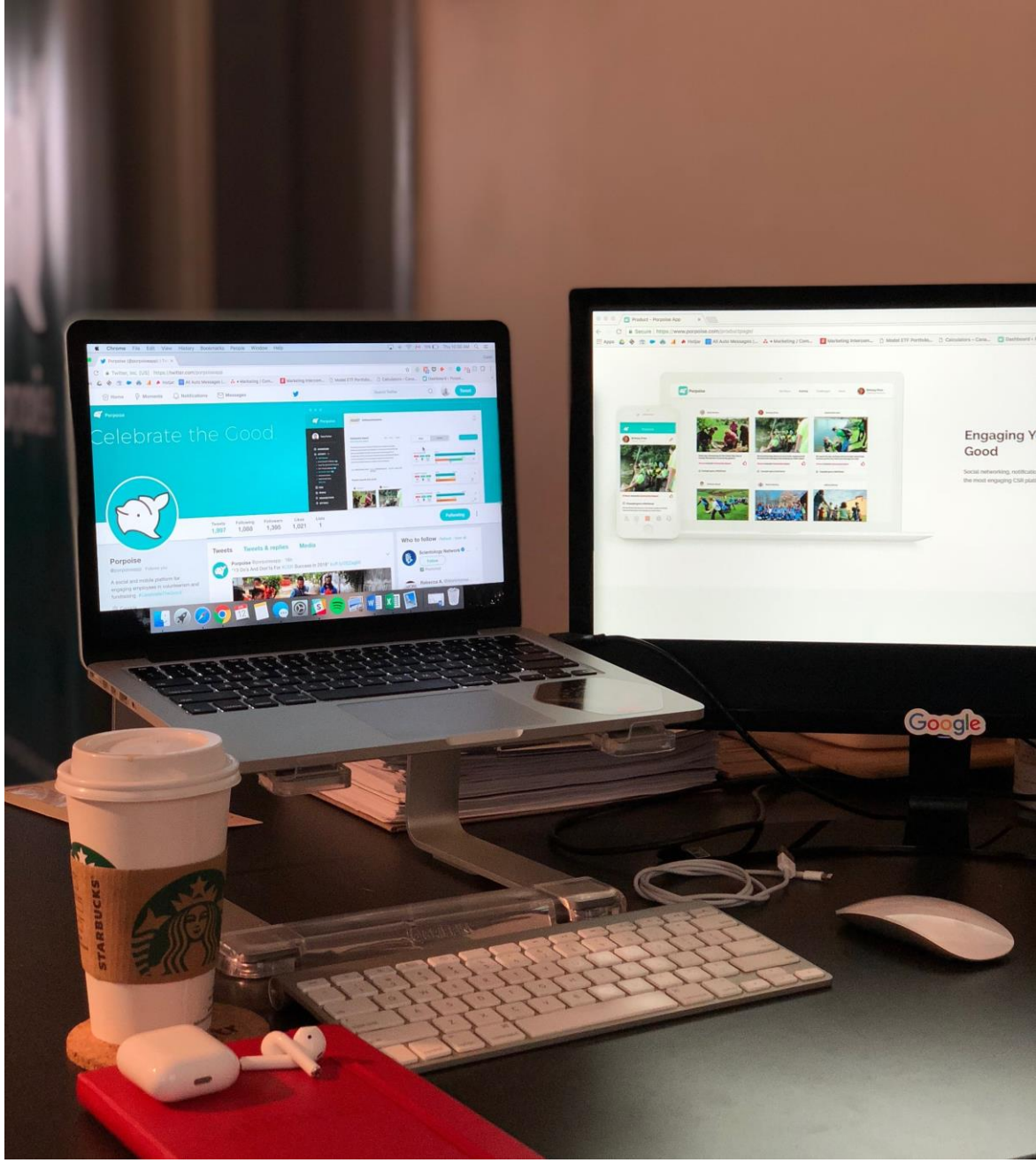
Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Objectives and Goals:

At the end of this module you will be able to:

- Know the main cyber-threats for SMEs before and during the pandemic.
- Manage tools to prevent cyber attacks.
- Use the most relevant tools to identify and react to cyber attacks.



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Index

Unit 1 **Cyber-threats for businesses before and during the pandemic**

1. Introduction
2. Main threats: what are they and where do they come from?
3. Top cyber-attacks on companies

Unit 2 **Main tools to prevent cyber risks**

1. Threat and vulnerability
2. How to prevent cyber attacks

Unit 3 **Main tools to identify cyber risks**

1. Antivirus software
2. Firewall
3. Virtual Private Network (VPN)
4. Vulnerability scanner

Erasmus+

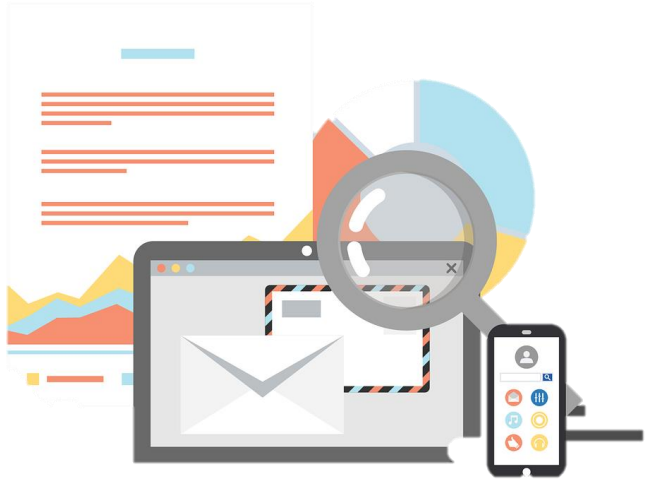
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Cyber threats for businesses before and during the pandemic

Section 1.1: Introduction

Whether it's confidential information, bank details or internal systems, there are many company assets that cybercriminals can target. Moreover, cybercriminals do not discriminate in the size of their targets, as they attack large companies as well as SMEs and the self-employed. For all these reasons, and to avoid suffering a security incident that could affect business continuity, it is vital to know the main fraudulent techniques, how to prevent them and what to do if you have been a victim of one of them.

With the Covid-19, hundreds of thousands or millions of people had to start working from home, with passwords, cloud, videoconferencing, encrypted access to the company's application. Pretending to be in the office but with their Wi-Fi cuts out, with their private computer and that outdated antivirus that does little to protect them. A study by Deloitte shows that 21 per cent of companies acknowledged that they were not at all or little prepared for the leap.



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

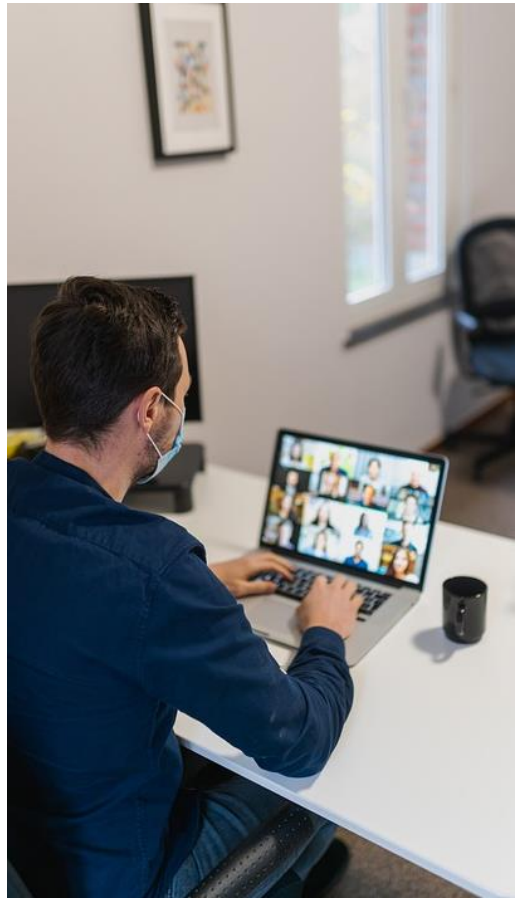
Unit 1: Cyber threats for businesses before and during the pandemic

Section 1.1: Introduction

The exploitation of security vulnerabilities opened up by teleworking impacts all countries almost equally. These incidents are being replicated throughout the first world and are mainly hitting companies with money.

Experts point out that criminals during the health emergency are adapting to the context of the coronavirus in the same way as they do on the occasion of Black Friday, the Olympics or the death of a celebrity, reorienting their actions by using the pandemic as a lure.

At the beginning of the pandemic, there were incidents related to health product fraud, subsidies to companies and the unemployed, and services used massively during confinement. In the late 2020s, others appeared related to restrictive measures being put in place in different countries.



The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.1: Introduction

Google reported in April 2020 that it was blocking an average of 18 million emails a day that referred to the coronavirus for deception. And of course, there were those who clicked on the cursed link disguised as something else and put the entire company in check through its mailing list.

It is one thing for companies to invest in protecting themselves in terms of cybersecurity, but it is another for their employees to be ready to know what to do and what not to do.

In a typical working day, many circumstances require urgency and immediacy: billing periods, fixed deadlines... cybercriminals know this and use it to trick us with everyday things like downloading an attachment.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.2: Main threats: what are they and where do they come from?

Cybercriminals have many tools in their arsenal to breach corporate security. Knowing how they do this can be a crucial factor when falling victim to a security incident. The following list shows the major security incidents that can affect businesses.

- Malicious code infections of systems, work computers or mobile devices. Such incidents, mostly initiated via email, compromised or malicious websites, SMS or social networks, can also result in infected resources becoming part of a botnet.

- Intrusions or intrusion attempts are caused by exploiting known vulnerabilities, use attacks, and credential breaches, leading to compromised accounts with or without administrator privileges and compromised applications or services. If the compromised service is the website, this may lead to incidents such as phishing or malware distribution, among others. This may also include incidents of theft through unauthorised access to physical facilities.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.2: Main threats: what are they and where do they come from?

- Availability failures through DoS (denial of service) attacks can affect the organisation's different resources (networks, servers, work equipment, etc.) and make their regular operation impossible. This type of incident also includes those caused by sabotage or physical attacks on resources or infrastructures and other types of unintentional interruptions of external origin.

- Data compromise results from unauthorised access to or modification of information (e.g. through encryption by ransomware). These incidents also include those that cause deletion, loss or leakage of data and may be caused intentionally (through theft or compromise of credentials) or by a failure of the devices that store them.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.2: Main threats: what are they and where do they come from?

- Fraud: caused mainly through impersonation of legitimate entities, to deceive users for financial gain, or through phishing attacks, to obtain private credentials for access to means of payment. Incidents related to the unauthorised use of resources can also be found here, with the aim of carrying out fraudulent campaigns against other users, such as hosting phishing campaigns on the corporate website.

- Other:
  - **Spamming:** unsolicited emails where the recipient of the content has not given permission to receive such messages. This type of message does not usually violate the company's security, as its purpose is usually to promote products or services, but in cases where there is a large volume of spam, it can be annoying for users.
  - **Network scanning**, which aims to discover technologies and systems used by the company. Scanning is usually part of the stage where cybercriminals obtain as much information as possible about a victim before perpetrating the attack.
  - **Packet analysis** (sniffing), to observe network traffic and analyse it in order to discover confidential information and tools used by the company.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.2: Main threats: what are they and where do they come from?

- **Social networks**. We cannot forget social networks because of their extraordinary relevance nowadays. The cybercriminal can impersonate the attacked company by using a profile almost identical to yours. In this way, he would have access to information about users, suppliers, etc. He could also make numerous negative comments to discredit the company by damaging its reputation.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.3: Top cyber-attacks on companies

The progressive digitalisation of companies and the increased use of the internet and smart devices have changed how many organisations work. This rapid transformation and the emergence of new technologies has also meant that cybercriminals have adapted their methods to the new scenario.

Despite the cybersecurity measures and improvements that are implemented every day in applications and browsers, cybercriminals try to avoid these protections to achieve their goals, going after the most crucial point in a company's cybersecurity chain: people. To do so, they take advantage of their lack of knowledge and the use of social engineering, seeking to breach the wall that defends the company from external threats.

Incidents originate mainly through email or websites can lead to financial loss, lack of information or reputational damage, putting the company's continuity at serious risk.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.3: Top cyber-attacks on companies

Most common online scams

Email spoofing.

Cybercriminals impersonate an organisation or individual by sending an email from a fake sender.

They send phishing emails.

They steal login credentials and banking information.

Spread malware, such as ransomware, or try to make your devices be part of a botnet.

Steal confidential company information.

They perform any action that could be profitable for them.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.3: Top cyber-attacks on companies

Most common online scams

Sextortion
The cybercriminal blackmails the victim with a supposed intimate video.

They use several social engineering tricks to put the victim on alert, such as a payment deadline.

Supplier impersonation.
The cybercriminal impersonates a company's supplier and asks to change the account number.

They often use emails that look very similar to those of the legitimate provider.

They create domain names very similar to the legitimate ones, a technique known as cybersquatting.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.3: Top cyber-attacks on companies

Most common online scams

Hot-Linking.
Use your web resources on a fraudulent website.

Cybercriminals generally use images to impersonate a product and benefit from your brand and reputation.

Brand and corporate image impersonation.

Cybercriminals create a copy of the legitimate website.

The fraudulent website sells products or services that it never ships.

They often use domain names similar to legitimate ones to deceive users.

Failure to detect this threat in time can lead to severe damage to your customers and your company's image.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 1: Cyberthreats for businesses before and during the pandemic

Section 1.3: Top cyber-attacks on companies

Most common online scams

E-skimming

Cybercriminals steal banking and personal information from users of legitimate online shops; **your online shop could be one of them**.

They use vulnerabilities, misconfigurations, or previous infections to introduce the malicious software that steals the information.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 2: Main tools to prevent cyber risks

Section 2.1: Threat and vulnerability

Concepts such as vulnerability and threat are closely related in the context of cyber-attacks.

In the IT area, we could consider a vulnerable system as one susceptible to a certain degree of damage, generally due to its own causes (lack of updates, low protection against viruses, etc.).

In many cases, in the enterprise, it is the user himself who creates the vulnerability or unintentionally facilitates the threat. Cybercriminals know this, considering users to be the weakest links in the chain, and therefore the most susceptible to threats and attacks.
We could affirm that the user is vulnerable to social engineering deception. But assuming that everyone is vulnerable is incorrect since there are no people who are 'invulnerable' to fraud, but rather well-trained and aware teams that can avoid it.

We also have to consider that a threat can become a vulnerability if the appropriate security measures are not applied through patches or software updates and adequate protection tools (antivirus, antimalware, etc.).

Erasmus+

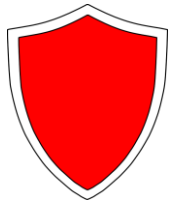
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: Main tools to prevent cyber risks

Section 2.1: Threat and vulnerability

Some examples to understand the scope of each concept:

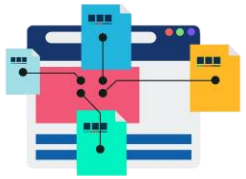
Online store without adequate protection measures



Not exempt from attack

THREATS

Man-in-the-middle attack
Zero-day explotation
Denial-of-service attack
Cross-site scripting
SQL injection
Social engineering attack

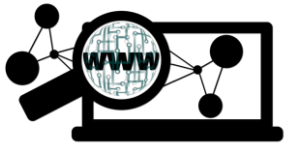


An updated website with appropriate security features

Protected against main threats

There is still some **risk**

Social engineering attack



A corporate website with appropriate security features

Protected against main threats

With trained and aware workers

Optimized protection

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 2: Main tools to prevent cyber risks

Section 2.2: How to prevent cyber attacks

Although there is no fail-safe method, we can prevent possible threats in the company if we raise awareness among the team, instructing them in the safe use of the technologies through training and prevention campaigns. Letting them know that any strange behaviour they may detect in day-to-day work should be reported as soon as possible to the personnel in charge of cybersecurity through the internal channels that the company makes available to them.

In addition, establishing an information channel, making employees aware of possible threats by means of information circulars (prevention), emails or any other means available to them will improve their awareness of these issues and put them on their guard against unforeseen risk situations. On the other hand, with regard to the company's IT equipment, its mission, among others, will be to update and keep the systems up to date and, if they have reached the end of their useful life (end of updates), to inform of the possible risk to the company and its employees of continuing in these conditions.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 2: Main tools to prevent cyber risks

Section 2.2: How to prevent cyber attacks

There is no 'magic recipe' to avoid a threat, but we can minimize them if we apply prevention as a general rule.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.1: Antivirus software

An antivirus is software used to prevent, scan for, detect and remove viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

An antivirus software starts by comparing your files and computer programs with a database of known malware types. Because hackers constantly create and distribute new viruses, antivirus software will also scan your computers for a new or unknown type of malware threat.

Integral virus protection software helps safeguard your files and hardware from malware, such as worms, Trojans and spyware, and can also offer additional protection, such as customizable firewalls and website blocking.

We can choose from a large number of antivirus products on the market, both free and paid. In addition, operating systems usually include a good antivirus. The essential is to have it always active and updated.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.2: Firewall

Firewalls are software programs or hardware devices that filter and examine the information coming through your Internet connection. They represent the first line of defence because they can prevent a malicious program or attacker from gaining access to your network and information before any potential damage is done.

We can identify 2 different kinds of firewalls, hardware firewalls and software firewalls.

Hardware firewalls are included in some routers. These firewalls monitor the traffic of all computers and devices that are connected to the router's network. Hardware firewalls provide essential security for the Internet of Things (IoT), such as smart thermostats and smart light bulbs. However, hardware firewalls only protect you at home, so if you take your computer to a café or use your device while travelling, you should look for a software firewall to keep your device protected.

Software firewalls help you stay protected in public places. Running as a program on your computer or device, they watch network traffic closely to help intercept malicious programming before it reaches your computer.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

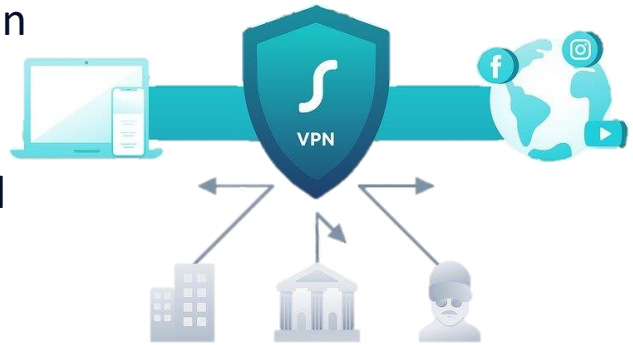
Unit 3: Main tools to identify cyber risks

Section 3.3: Virtual Private Network (VPN)

VPN stands for "Virtual Private Network", it is an encrypted connection over the Internet from a device to a network. VPNs encrypt your internet traffic and disguise your online identity. The encrypted connection helps ensure that sensitive data is safely transmitted. VPN makes it more difficult for third parties to track your activities online and steal data. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.The encryption takes place in real-time.

How does a VPN work?

A VPN extends a corporate network through encrypted connections made over the Internet. A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work from home using a computer, smartphone and tablet and still securely connect to the corporate network.



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.3: Virtual Private Network (VPN)

What kind of VPNs are there?

- Remote access:

  A remote-access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones.
  The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. Access is guarded with a username and password.

- Site-to-site VPN:

  It is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources. A site-to-site VPN is useful if you have multiple locations in your company, and distance makes it impractical to have direct network connections between these offices.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.3: Virtual Private Network (VPN)

Connect to a VPN in Windows 10

1. Create a VPN Profile

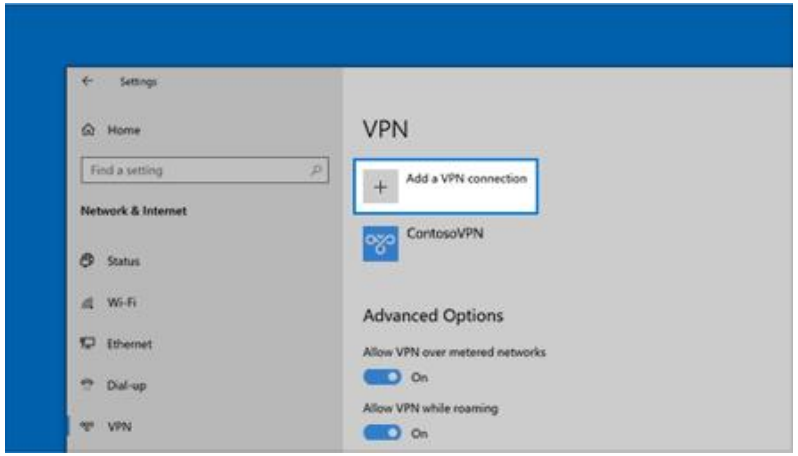


Image: https://support.microsoft.com

1. Select the **Start** button, then select **Settings** > **Network & Internet** > **VPN** > **Add a VPN connection**.

2. In **Add a VPN connection**, do the following:
   - For **VPN provider**, choose **Windows (built-in)**.
   - In the **Connection name** box, enter a name you'll recognize (for example, My Personal VPN). This is the VPN connection name you'll look for when connecting.
   - In the **Server name or address** box, enter the address for the VPN server.
   - For **VPN type**, choose the type of VPN connection you want to create. You'll need to know which kind of VPN connection your company or VPN service uses.
   - For **Type of sign-in info**, choose the type of sign-in info (or credentials) to use. This might be a username and password, one-time password, certificate, or a smart card if you're connecting to a VPN for work. Enter your username and password in the respective boxes (if required).
3. Select **Save**.

4. If you need to edit the VPN connection info or specify additional settings, such as proxy settings, choose the VPN connection and then select **Advanced options**.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.3: Virtual Private Network (VPN)

Connect to a VPN in Windows 10

2. Connect to a VPN

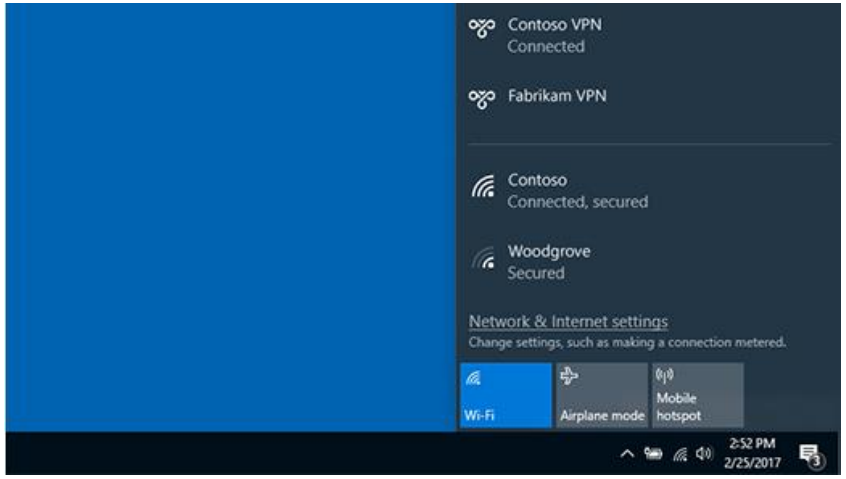


Image: https://support.microsoft.com

When you have a VPN profile, you're ready to connect.

1. On the far right of the taskbar, select the **Network** icon (either or).
2. Select the VPN connection you want to use, then do either of the following depending on what happens when you select the VPN connection:
    - If the Connect button displays under the VPN connection, select **Connect**.
    - If the VPN section in Settings opens, select the VPN connection there, then select **Connect**.
3. If you're prompted, enter your username and password or other sign-in info.

When connected, the VPN connection name will display **Connected** underneath it. To see if you're connected to the VPN while you're doing things on your PC, select the **Network** icon (either or) on the far right of the taskbar, then see if the VPN connection says **Connected**.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Unit 3: Main tools to identify cyber risks

Section 3.4: Vulnerability Scanner

All companies, large and small, store data and information. If we want to keep the network as secure as possible, without any vulnerabilities; therefore, we need to identify weaknesses in our network.

Vulnerability scanners are valuable tools that search for and report on what known vulnerabilities are present in an organization's IT infrastructure.
The vulnerability scanner is an integral component of a vulnerability management program, which has one overarching goal – to protect the organization from breaches and the exposure of sensitive data.

Companies can use different vulnerability scanners depending on the type of scanning they need.

- Network-based scanners to scan the wired or wireless corporate network.
- Host-based scanners to scan for threats on servers.
- Wireless scanners to identify breaches in wireless access points.
- Database scans to identify weaknesses in the database.
- Application scanning to detect vulnerabilities in software or web applications.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Bibliography and relevant links

Incibe. National Institute of Cybersecurity> **Awareness kit for companies.**

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

CoreSecurity > **Top 14 Vulnerability Scanners for Cybersecurity Professionals**

https://www.coresecurity.com/blog/top-14-vulnerability-scanners-cybersecurity-professionals

Redlegg > **WHAT IS VULNERABILITY SCANNING, AND HOW DOES IT WORK?**

https://www.redlegg.com/blog/what-is-vulnerability-scanning-and-how-does-it-work

Kaspersky > **What is VPN? How It Works, Types of VPN**

https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Microsoft > **Connect to a VPN in Windows 10**

https://support.microsoft.com/en-us/windows/connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c

Forbes> **New Dangers Of Working From Home: Cybersecurity Risks**

https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/?sh=1d8724b022fb

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.

Thank you for your attention

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect 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.