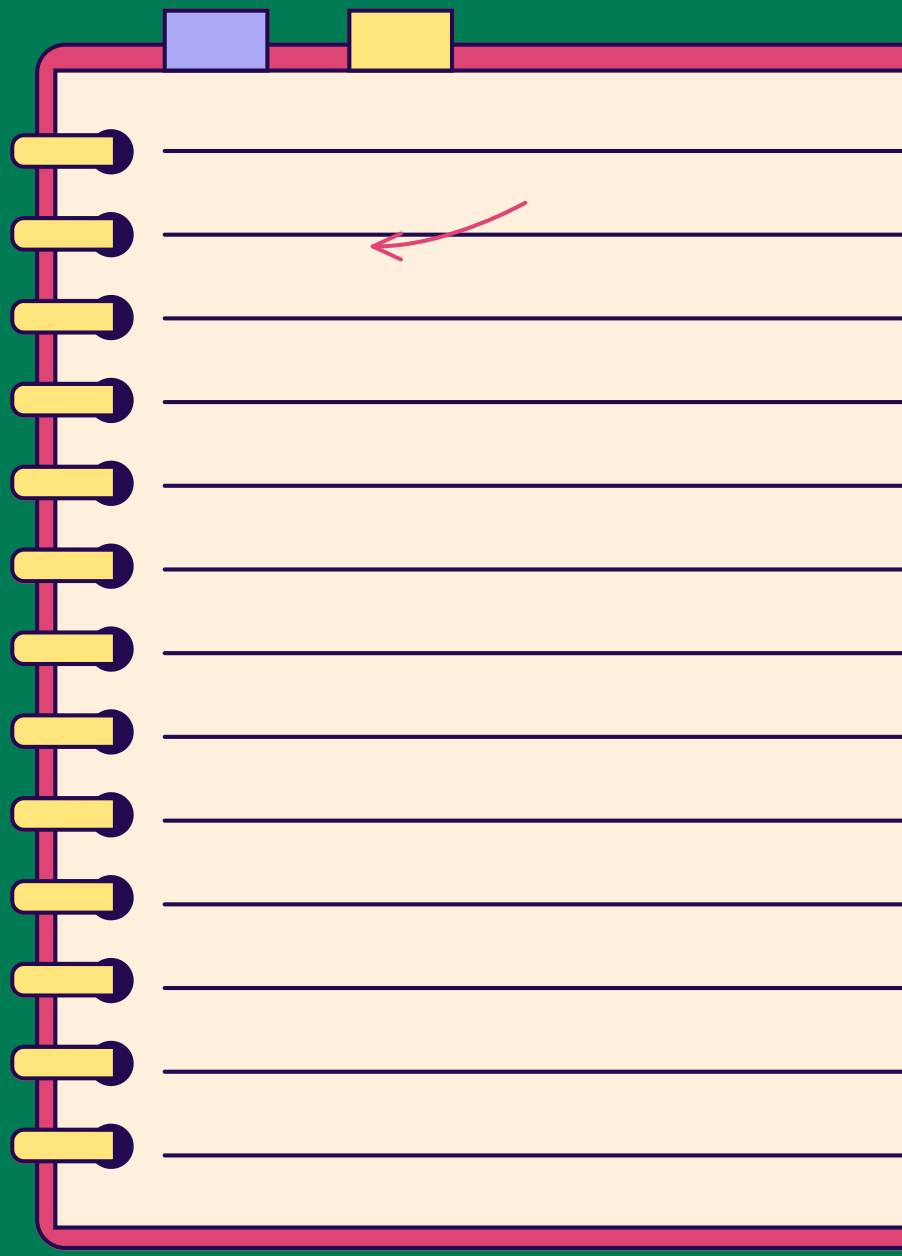
MODULE 12 - ONLINE SCAMS

CHAPTER 2

HOW TO PROTECT YOURSELF AGAINST SCAMS

Skills to Connect



INTRODUCTION

In this chapter, we'll explore best practices for protecting yourself from online scams. You'll learn essential security tools like antivirus and firewalls, as well as simple habits you can adopt to keep your devices secure. You'll also learn how to use additional protection methods, like two-factor authentication, to keep your online accounts safe. By the end of this chapter, you'll know how to strengthen your defenses against cybercriminals.

1 SOME TERMS TO CLARIFY

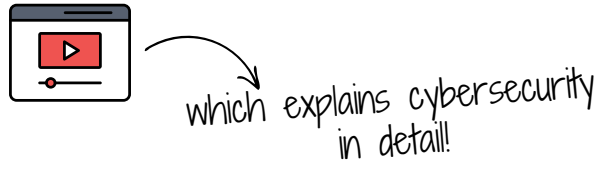
WHAT IS CYBERSECURITY?

Cybersecurity refers to the set of strategies and technologies implemented to protect computer systems, networks and data against any form of threat, whether malicious or accidental.

- Its main objective is to prevent unauthorized access, theft, corruption or damage to information and IT infrastructure. This includes protecting personal data, securing online transactions, as well as managing risks related to malware, phishing attacks and security breaches.

- In practice, cybersecurity relies on technical measures such as firewalls, antivirus software, and multi-factor authentication. It also includes organizational aspects, such as user training and implementing robust security policies to ensure appropriate risk management.

Watch the video



1 SOME TERM TO CLARIFY

WHAT IS A HACKER?

- **Hacker:** Originally, a hacker was someone who had a deep understanding of computer systems and software. They were technology enthusiasts who enjoyed exploring and understanding complex systems. Hackers often developed advanced programming skills and were able to find creative solutions to technical problems. Within this community, "hacker" generally had a positive connotation and was associated with curiosity and technical competence.
  Now, this term is often used to describe someone who uses technical skills to access computer systems without permission and with malicious intent. Hackers can be involved in activities such as stealing information, compromising systems, spreading malware, among others. Now, hackers are generally perceived negatively and are associated with illegal and harmful activities.

2 PROTECT YOURSELF AGAINST SCAMS

HOW TO DO IT?

STEP 1: PROTECT YOUR DEVICES

First of all, it is essential to protect our computers and mobile devices from cyber attacks. This includes installing reliable antivirus programs and firewalls, as well as keeping all software up to date. Many cyber attacks exploit vulnerabilities in outdated software, so keeping the system up to date is essential to prevent intrusions.

- **Firewall:** A firewall is a security system that acts as a barrier to protect a computer network. It monitors internet connections and decides what data can enter or leave, in order to block threats or attacks. Basically, it prevents bad connections from getting through and protects your computer or network from dangers.

- **Antivirus:** An antivirus is a program designed to detect and remove viruses and other malware from your computer. It protects your device by scanning files and preventing threats from infecting your system. It also plays a preventative role by stopping viruses before they cause damage.

MODULE ALERT

Find out more about protecting your devices in Module 1!

2 PROTECT YOURSELF AGAINST SCAMS

HOW TO DO IT?

STEP 2: PROTECT YOUR ACCOUNTS

Protecting our online accounts is very important. Many people use simple passwords or the same passwords for multiple accounts, making it easier for hackers to steal them.

- It is essential to have strong and different passwords for each account.

MODULE ALERT

Find out how to choose a password in Module 5 on Data Management!

- We recommend to use **two-factor authentication** when possible:
  - Two-factor authentication is an additional security method to protect your online accounts. Instead of just your password to log in, this method asks you for two pieces of information to verify your identity.
  - The first step is to enter your password, as usual. The second step is where two-factor authentication comes in: an additional code is sent to you. This code can be sent via SMS to your phone, via email, or it can be generated by an app like Google Authenticator.
  - This code is usually valid for a short time and is unique to each login. Even if someone manages to steal your password, they will be unable to log in without the second code. This double check ensures that only you can access your account, even if someone else knows your password.

More and more applications and websites require two-factor authentication, such as Facebook, Google & Microsoft

2 PROTECT YOURSELF AGAINST SCAMS

HOW TO DO IT?

STEP 3: PROTECT YOUR DATA

It's crucial to be aware of how we share our personal information online and take steps to protect it. That means limiting the information we share on social media and other sites, and being extra vigilant when filling out online forms. Hackers often target sensitive data like credit card numbers, Social Security numbers, and dates of birth, which can be used for identity theft or other forms of fraud.

Protecting our personal data is therefore an essential step in preventing online scams. By reducing the information we share and being attentive to the security of the websites we use, we can minimize the risk of being a victim of scams.

MODULE ALERT

Learn how to protect your data by following Module 1 on Device Protection!

TO REMEMBER!

Habits to adopt to protect yourself from online scams:

- Learn to recognize the different types of scams and the signs to look out for to avoid falling into the trap
- Protect your devices by updating your devices and installing firewalls and anti-virus software
- Protect your data and accounts by using strong passwords and using two-factor authentication.