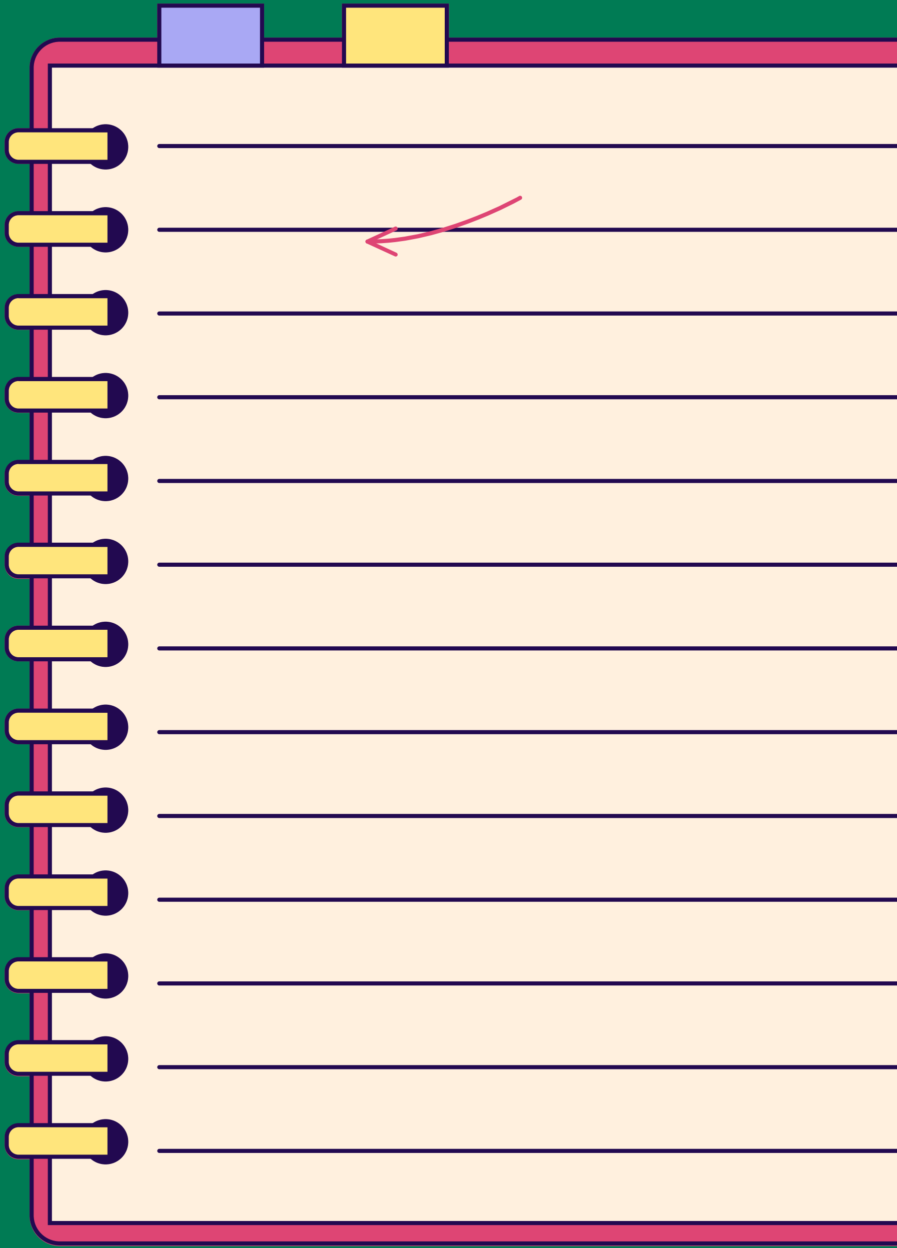
MODULE 1 - CHOOSING YOUR DEVICE
AND PROTECTING IT

CHAPTER 3

PROTECTING YOUR DEVICES DIGITALLY

Skills to Connect



INTRODUCTION

Protecting your devices digitally means ensuring that you keep your data safe and prevent any theft or hacking of your information. Since the explosion of digital technology and devices, digital hackers are constantly developing new strategies to obtain our data, or even "kidnap" it with a ransom.

It is therefore essential to protect your devices to prevent any inconvenience later on.

In this chapter, we will cover different topics: antiviruses, codes and other systems to lock your information and prevent anyone from accessing it, the importance of updates and checking whether we trust the sites with which we share our information.

Here we go!

1 ANTIVIRUS

EVERYTHING YOU NEED TO KNOW ABOUT ANTIVIRUSES!

WHAT IS AN ANTIVIRUS?

- An antivirus is a program designed to detect, neutralize or eradicate malware (viruses, Trojans, ransomware, spyware, etc.) from computing devices.
- It also plays a preventative role by preventing infections and enabling regular scans of your computer to spot suspicious files. A system without antivirus is like a house with an open door: it attracts unwanted intruders.
- An antivirus acts as a security guard, protecting your system from attacks.

WHY IS AN ANTIVIRUS NECESSARY?

- In 2019, one antivirus vendor reported detecting 2.6 million threats, that's huge! Securing your device is essential. In fact, any device connected to the internet is potentially at the mercy of attacks and cybercrime. But it doesn't stop there. A device can also be infected via a USB key or an external hard drive, which are themselves infected via another device. You can therefore infect others or be infected by others.
- Possible impacts include:
  - Computer disruption and slowdown.
  - Blocking, deleting or encrypting files in exchange for payment (ransomware).
  - Theft of personal data (bank details, work carried out).
  - Remote control of the computer.
  - Phishing to capture login or payment data.
  - Using the computer's processing power for malicious purposes.

MODULE ALERT

Learn more about online scams by clicking here!

1 L'ANTIVIRUS

EVERYTHING YOU NEED TO KNOW ABOUT ANTIVIRUSES!

HOW DOES AN ANTIVIRUS WORK?

- Antivirus programs use three main methods of detection:
  - Specific detection: It compares files on the computer with known malware databases to detect them.
  - Generic detection: Searches for variants of known viruses.
  - Heuristic detection: Identifies unknown viruses by analyzing program behavior.

HOW TO CHOOSE THE RIGHT ANTIVIRUS?

Important features:

- **Overall Protection:** Evaluate overall protection first before looking at additional features.
- **Test Results:** Check specific performance, especially for phishing.
- **Additional features:** Some antiviruses include tools like password managers or VPNs.
- **Only one antivirus:** Installing several antiviruses is counterproductive; they risk blocking each other.

1 L'ANTIVIRUS

EVERYTHING YOU NEED TO KNOW ABOUT ANTIVIRUSES!

HOW TO COMPARE DIFFERENT ANTIVIRUSES?

- Use an antivirus comparator (like Test Achat in Belgium for example)
- The operating system also plays a role. The results of antivirus tests are not always exactly the same for a Windows version or a macOS (Apple) version;
- For paid products, look for current promotions, depending on the number of devices you want to protect;
- Free products include advertising, which is more or less cumbersome.

System Requirements

- Check the minimum system requirements to avoid slowing down your device.

Popular brands

- Avast, AVG, Avira, Bitdefender, ESET, F-Secure, G Data, Kaspersky, McAfee, Microsoft, Norton, Panda Security, Sophos, Trend Micro.
- Some offer free versions with ads; paid versions offer customer support and less advertising.

Shopping tips

- Look for discounts when it comes to paid products.
- Uncheck auto-renew if you don't want it.
- Test a free version before committing financially, to see if it is easy to get started with and if you find it easy to use. This allows you to do an initial scan and analysis of your computer.

1 L'ANTIVIRUS

EVERYTHING YOU NEED TO KNOW ABOUT ANTIVIRUSES!

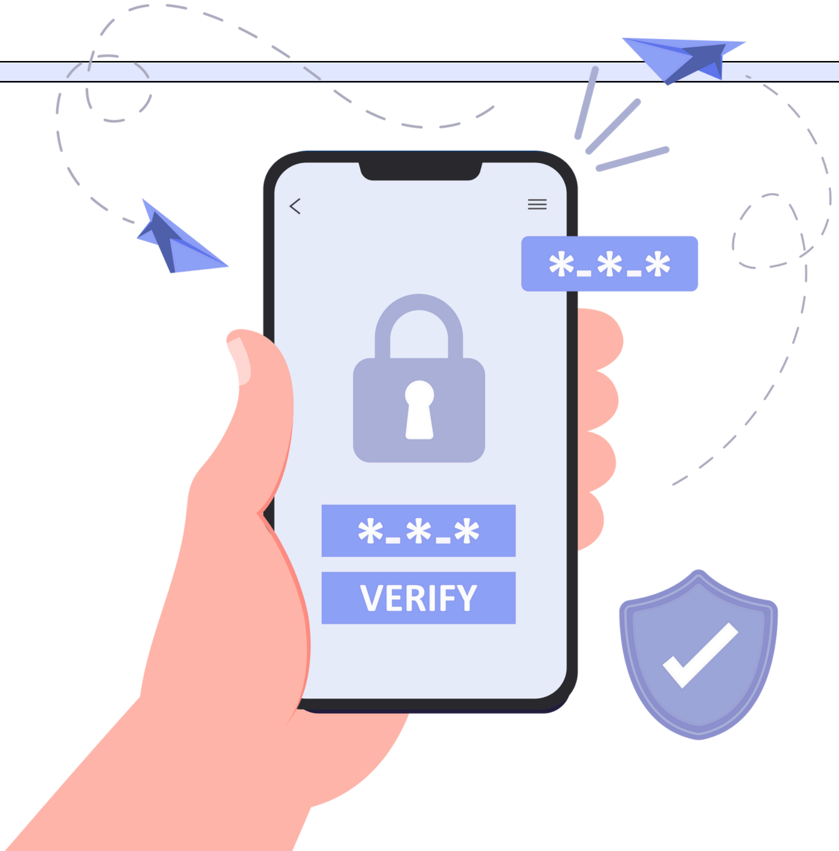
BEST PRACTICES FOR USING ANTIVIRUS

- **Scan Removable Media:** Scan USB drives and external hard drives to prevent contamination.
- **Quarantine suspicious files:** Avoid deleting them immediately, by placing them in quarantine you can verify their nature before making a decision.
- **Update regularly:** Make sure your antivirus is up to date before each scan. Enable automatic updates if possible.
- **Perform regular scans:** Schedule regular scans of your system to detect threats on time.
- **Cut off internet connection if infected:** This prevents malware from communicating data remotely.
- **Use strong passwords:** Change your passwords regularly and use complex passwords.
- **Avoid suspicious links:** Do not click on suspicious links in emails or unsecured websites.

2 SECURE APPS

WHY IS APP SECURITY IMPORTANT?

When you download apps to your phone, you may unknowingly expose your personal information. Some apps may even contain malware that steals your data or damages your device.
Here are some simple tips to protect yourself.



2 SECURE APPS

SAFETY TIPS FOR DOWNLOADING APPS

1. DOWNLOAD ONLY FROM OFFICIAL SOURCES

- Use official app stores like Google Play Store for Android or App Store for iPhone.
- Avoid unknown sites and app stores that may offer unverified apps.
- Do not download apps by clicking on links in unsolicited emails or text messages.
- Avoid doubtful websites that offer free or pirated applications.
- Example: If you receive a link via SMS to download a new health app, first check its legitimacy.

2. PAY ATTENTION TO THE PERMISSIONS REQUESTED

- When you install an app, it asks for permissions to access certain features of your phone.
- If an app asks for permissions that seem excessive, **be careful!**
- Example: A task management app shouldn't need access to your photos.

2 SECURE APPS

SAFETY TIPS FOR DOWNLOADING APPS

3. READ REVIEWS AND RATINGS

- Before downloading an app, look at what other users say about it.
- Be wary of apps with few or many negative reviews.
- Example: If you are looking for an application to track your journeys between your different beneficiaries, choose one with good reviews and there should be many of them.

4. UPDATE YOUR APPS REGULARLY

- Updates often fix security issues.
- Turn on automatic updates so you don't have to think about them.

5. BEWARE OF FREE APPS

- Some free apps may finance their services by displaying ads or containing spyware. Prefer apps from well-known publishers and with good ratings. For example, a free note-taking app could collect your data to sell to advertisers.

2 SECURE APPS

SAFETY TIPS FOR DOWNLOADING APPS

6. MONITOR YOUR PHONE'S PERFORMANCE

- If your phone suddenly becomes slow or acts strangely after installing an app, uninstall that app.
- In your phone settings, it is possible to check how much battery and data apps are using. If it seems too high, exit the page and/or uninstall the app

7. BEWARE OF FREEMIUM APPS!

- Some apps are free at first, but start charging after a trial period or require payments to unlock additional features. For example, an app becomes paid after a month of free use but will directly ask you to enter your bank details and will charge you later
- Read the terms of use carefully and check for hidden costs before installing an app.

3 CODES AND OTHER LOCKS

WHY IS THE SECURITY OF YOUR DEVICES IMPORTANT?

Mobile devices, such as phones and tablets, often contain sensitive personal information. Protecting these devices is essential to prevent this information from falling into the wrong hands.
Among the available protections, codes, fingerprints, etc. are locking methods: your device cannot be seen without being unlocked.

These prevent anyone from having access to your devices.

HERE ARE SOME SIMPLE TIPS TO SECURE YOUR DEVICES USING THESE LOCKING METHODS:

3 CODES AND OTHER LOCKS

WHY IS THE SECURITY OF YOUR DEVICES IMPORTANT?

WHAT IS A PASSWORD OR PIN CODE?

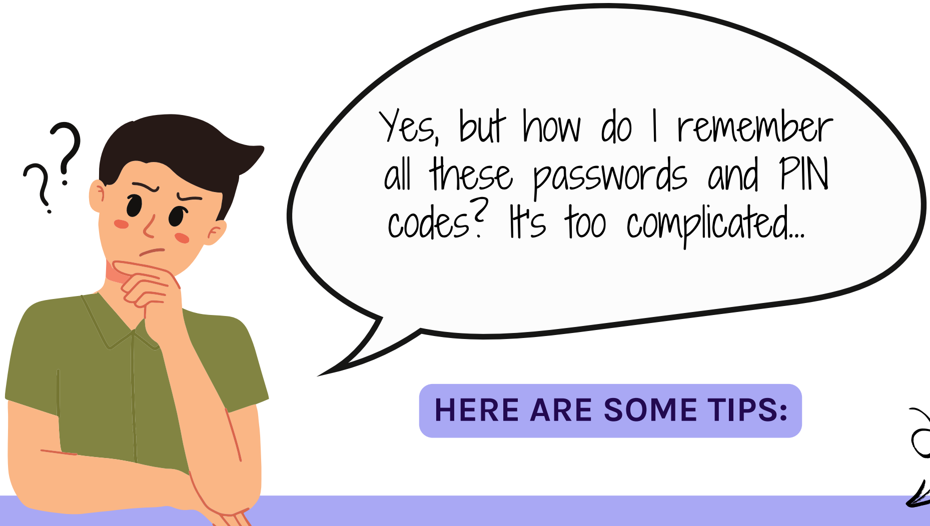
- A password is a series of letters, numbers, and sometimes symbols that you create to protect your device.
- A PIN is a numeric code (often 4 or 6 digits) that you enter to unlock your device.
- They prevent unauthorized people from accessing your personal information if they pick up your phone.

HOW TO CREATE A PASSWORD?

- Creating a strong password or PIN code is the best way to ensure the security of your device. The more complex it is, the harder it will be to discover it. A pin code of “1234” is much too simple. Similarly, it is advisable not to use a password that is too simple, for example the name of your children, because it is too easy for hackers to find this information and unlock your devices.
- **Criteria for a good password or PIN code:**
  - Strong: Use a combination of letters (upper and lower case), numbers, and symbols. For example, "A!d3_@D0m1c1l3".
  - Length: The longer the password, the better. Try to use at least 12 characters.
  - Complexity: Mix different types of characters (letters, numbers, symbols).
  - Diversity: Avoid using the same password for multiple accounts.
  - PIN Code: Use a 6-digit code instead of a 4-digit code for added security. For example, "482193" is much more secure than "1111".

4 LOCK YOUR DEVICES

USE A PASSWORD OR PIN CODE


Yes, but how do I remember all these passwords and PIN codes? It's too complicated...

HERE ARE SOME TIPS:

WAYS TO REMEMBER YOUR PASSWORDS AND PINS

- **Memorization:** Create easy-to-remember sentences and use the first letters of each word. For example: "My Dog Bruno Loves Playing In The Park!" becomes "MDB@LPIT_P!".
- **Password Manager:** Use a password manager to store and generate strong, complex passwords. You only need to remember one master password.
- **Secure Notes:** If you absolutely must write down your passwords, don't spell them entirely, use hints or codes that only you understand and keep them in a secure place (eg. Bruno's favorite activity: playing in the park)

4 LOCK YOUR DEVICES

USE FINGERPRINT

FINGERPRINT

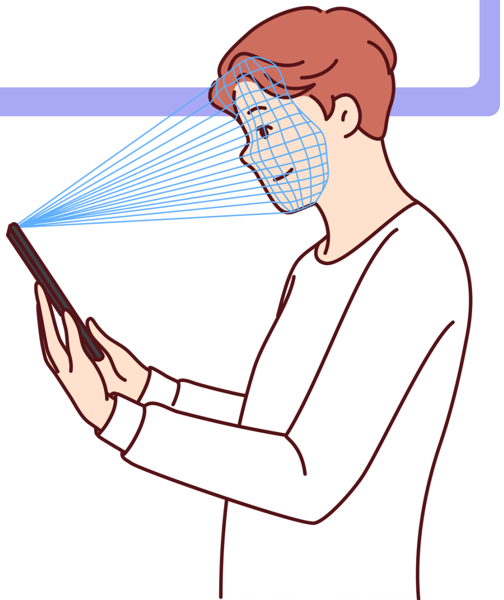
- **What is fingerprint?**
  - It is a security method that uses your fingerprint to unlock your device.
- **Why use it?**
  - It’s quick and convenient. Just place your finger on the sensor to unlock your device.
  - It's more secure than simple passwords or PINs because every fingerprint is unique.
- **How to activate it?**
  - Go to your phone settings.
  - Look for security or biometric options.
  - Follow the instructions to register your fingerprint.

4 LOCK YOUR DEVICES

USING FACIAL RECOGNITION

FACIAL RECOGNITION

- **What is facial recognition?**
  - It is a security method that uses a camera to recognize your face and unlock your device.
- **Why use it?**
  - Like fingerprint, it's quick and convenient.
  - It's secure because it's difficult for someone to fake your face.
- **How to activate it?**
  - Go to your phone settings.
  - Look for security or biometric options.
  - Follow the instructions to register your face.



4

LOCK YOUR DEVICES

GENERAL TIPS FOR DEVICE SAFETY

1

Do not share your passwords or PIN codes!

Keep this information to yourself to protect your data.

2

Change your passwords regularly!

Update your passwords from time to time for added security.

3

Use extra protection for sensitive applications!

If you have apps that contain sensitive information (like banking apps), add an extra layer of security (like a password or fingerprint to access those apps).

4

Be aware of unsecured environments!

Avoid unlocking your phone or entering your passwords in public where someone could see what you are doing.

5

2-FACTOR AUTHENTICATION

WHAT IS 2-FACTOR AUTHENTICATION?

- 2-factor authentication (or 2FA) is a security method that adds an extra layer of protection when logging into your online accounts.
- It requires not only a password, but also a second verification element, often called a "factor," which is something you have (like your phone) or something you are (like a fingerprint) that will help prove it's you.

IN SUMMARY: YOU IDENTIFY YOURSELF TWICE INSTEAD OF ONCE!

5

2-FACTOR AUTHENTICATION

WHY IMPLEMENT 2-FACTOR AUTHENTICATION?

STRENGTHENING SECURITY

- Even if someone figures out your password, it will be difficult for them to access your account without the second factor. This greatly reduces the risk of hacking, as an attacker would need both your password and the second factor.
- Passwords can be stolen or guessed, but the second factor, usually a physical piece of information you possess, is much harder to compromise. You can rest easier knowing your accounts are better protected.

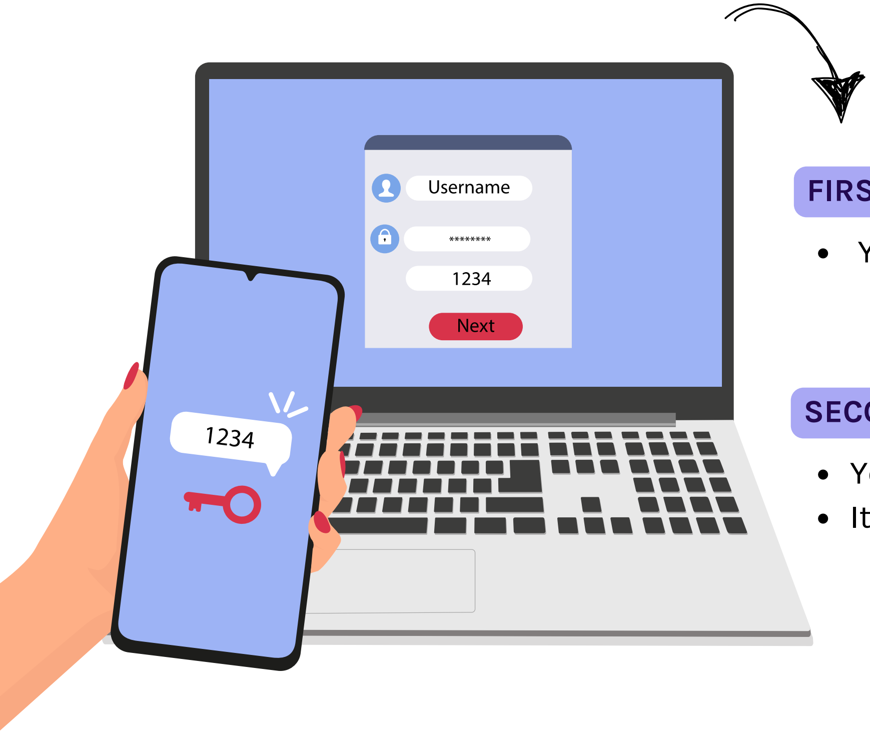
PROTECTING YOUR SENSITIVE DATA

- Your data is much more secure with two-factor authentication than with a single password. Think of your bank accounts, emails, etc.
- As a home assistant, you may have (access to) personal and sensitive information on your phone or computer (such as appointments, notes on beneficiaries, etc.). It is therefore important to do everything possible to ensure that this data is protected!

5

2-FACTOR AUTHENTICATION

WHY IMPLEMENT 2-FACTOR AUTHENTICATION?



FIRST STEP:

- You enter your username and password as usual.

SECOND STEP:

- You are prompted to provide a second verification element.
- It can be:
    - **Code sent by SMS:** You receive a code on your phone that you must enter.
    - **Authenticator app:** An app like Google Authenticator or Microsoft Authenticator generates a one-time, time-limited code.
    - **Physical security key:** A small device that you insert into your USB port.
    - **Biometric recognition:** Using your fingerprint or facial recognition.

5

2-FACTOR AUTHENTICATION

HOW TO ENABLE 2-FACTOR AUTHENTICATION?

ON A GOOGLE ACCOUNT

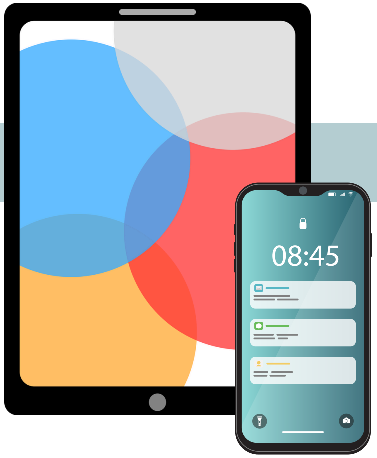
- Go to your Google account settings.
- Select “Security” then “Two-step verification”.
- Follow the instructions to add your phone number or an authenticator app.

For Android (smartphone and tablet)

ON AN ICLOUD ACCOUNT

- Go to “Settings”, then click on your name at the top.
- Select “Password & Security” then “Enable 2-Factor Authentication”.
- Follow the steps to configure.

For Apple (smartphone and tablet)



ON A WINDOWS COMPUTER:

- Go to your Microsoft account website.
- Under “Security,” select “More security options” and then “Set up 2-factor authentication.”
- Choose your preferred method and follow the instructions.

6 UPDATES

WHAT ARE UPDATES?

- Updates to your phone, computer, or tablet are like regular doctor visits. They're crucial to maintaining the security and performance of your device. They fix security vulnerabilities, add new features, and improve app stability.
- For example, if you use an app to travel in order to visit the supported people, an update could correct a bug that was wasting your time by offering poorly optimized routes or not taking into account certain changes.
- Consider turning on automatic updates to ensure your device stays secure without you having to think about it.

6 UPDATES

HOW TO ENABLE UPDATES?

FOR ANDROID DEVICES

- Tap the “Settings” icon on your phone.
- Scroll down and tap “System”.
- Tap “Advanced” and then “System Updates”.
- Tap “Check for updates”. If an update is available, follow the instructions to install it.
- Make sure the automatic updates option is enabled.

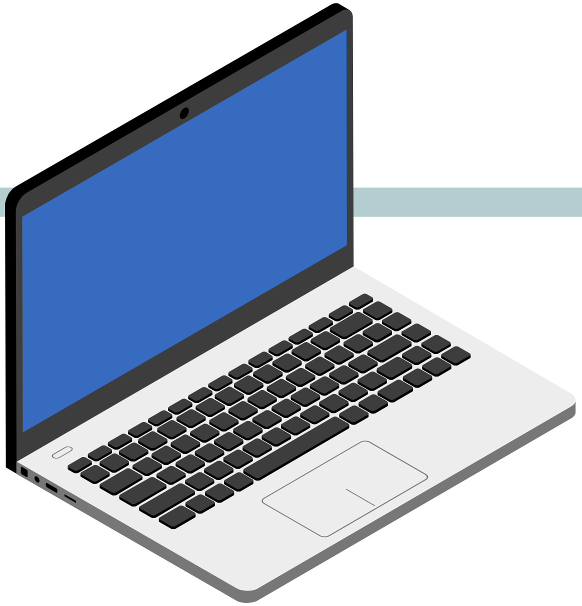
6

UPDATES

HOW TO ENABLE UPDATES?

FOR WINDOWS COMPUTERS:

- Click on the "Start" menu and select the "Settings" icon (cogwheel).
- Click on “Update & Security”.
- Click on “Windows Update” in the left menu.
- Click "Check for updates". If updates are available, they will install automatically.
- Make sure automatic updates are turned on. Windows usually installs updates automatically by default.



6

UPDATES

HOW TO ENABLE UPDATES?

FOR IOS (APPLE) DEVICES:

- Tap the “Settings” icon.
- Scroll down and tap “General”.
- Tap “Software Update”.
- Tap “Automatic Updates” and turn on “Download iOS Updates” and “Install iOS Updates”.

7 THE “LOCALIZE” FUNCTION

WHAT IS IT?

- The "Localize" function is essential to help find your phone. It is even more relevant when you have a mobile job. Imagine that you lose your phone on the way between two homes. With this function, you can locate it on a map, make it ring to find it or even lock access remotely to protect your sensitive data and that of the supported people.
- Enable this feature in your phone settings to gain peace of mind and keep your business information secure.

7

THE “LOCALIZE” FUNCTION

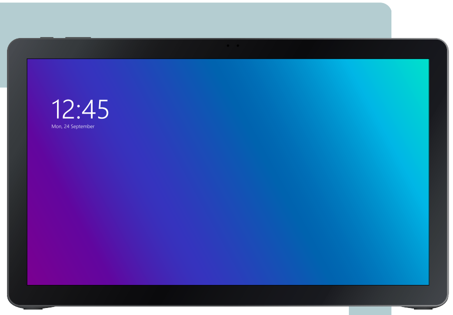
HOW TO ENABLE UPDATES?

FOR ANDROID SMARTPHONES:

- Tap the “Settings” icon.
- Tap your name at the top of the screen.
- Tap “Find My” then “Find My iPhone”
- Turn on “Find My iPhone” and “Send Last Location”.

FOR ANDROID TABLETS:

- Tap the “Settings” icon.
- Scroll down and tap “Security”.
- Tap “Find my device”.
- Make sure the feature is enabled.



FOR MACOS (APPLE) COMPUTERS

- Click on the “Start” menu and select the “Settings” icon.
- Click on “Update & Security”.
- Click on “Find my device” in the left menu.
- Click “Edit” under “Find My Device is turned off” and turn the feature on.

7 THE “LOCALIZE” FUNCTION

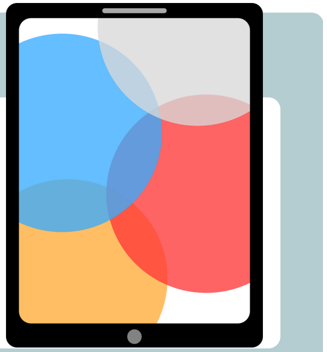
HOW TO ENABLE UPDATES?

FOR IOS (APPLE) SMARTPHONES:

- Tap the “Settings” icon.
- Tap your name at the top of the screen.
- Tap “Find My” then “Find My iPhone”
- Turn on “Find My iPhone” and “Send Last Location”.

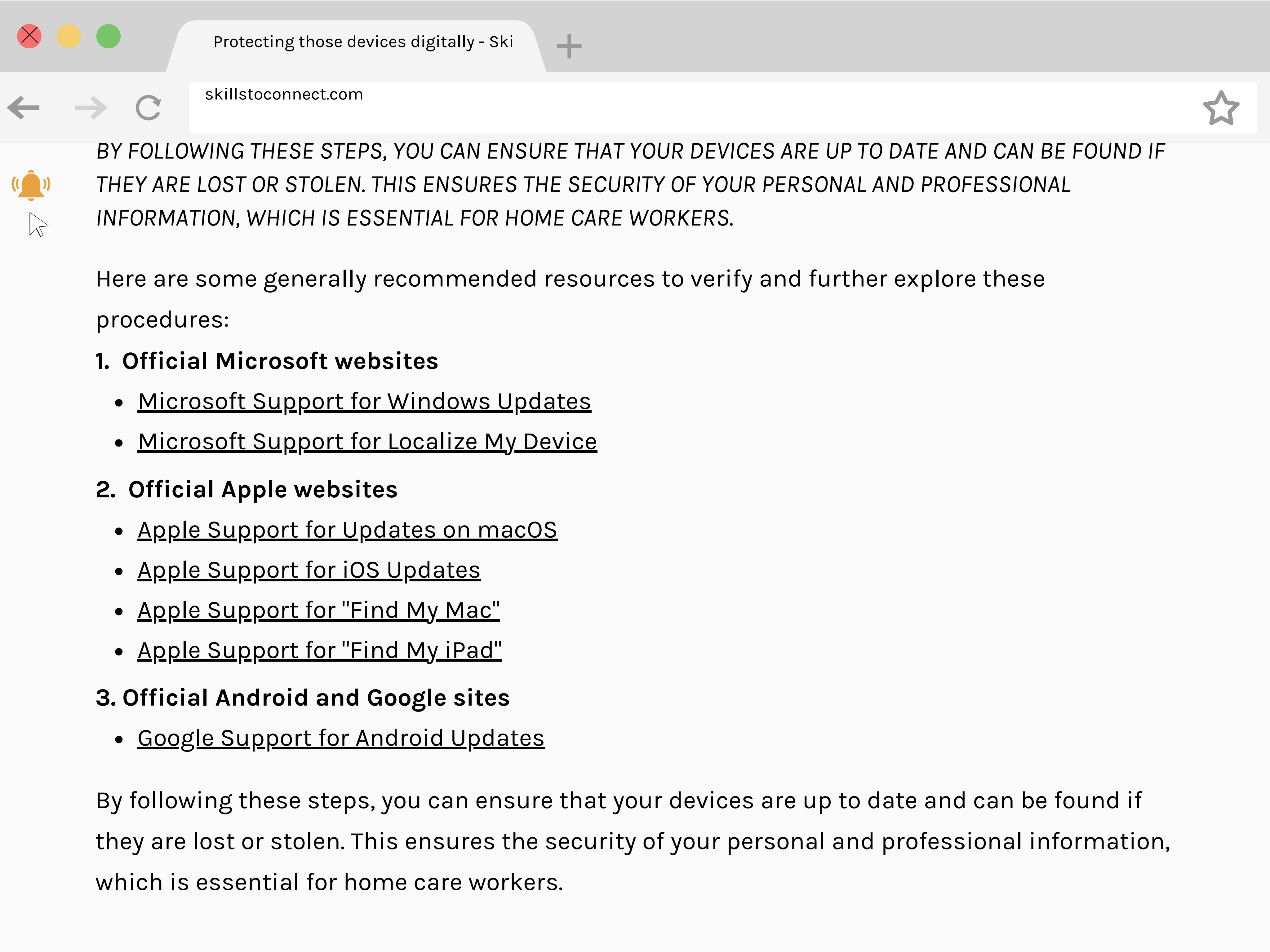
FOR IOS (APPLE) TABLETS:

- Tap the “Settings” icon.
- Tap your name at the top of the screen.
- Tap “Find My” and then “Find My iPad”.
- Turn on “Find My iPad” and “Send Last Location”.



FOR MACOS (APPLE) COMPUTERS

- Click on the “Apple” menu at the top left of the screen and select “System Preferences”.
- Click on “Apple ID” then “iCloud”.
- Check the box next to “Find My Mac”. You may need to sign in with your Apple ID.



BY FOLLOWING THESE STEPS, YOU CAN ENSURE THAT YOUR DEVICES ARE UP TO DATE AND CAN BE FOUND IF THEY ARE LOST OR STOLEN. THIS ENSURES THE SECURITY OF YOUR PERSONAL AND PROFESSIONAL INFORMATION, WHICH IS ESSENTIAL FOR HOME CARE WORKERS.

Here are some generally recommended resources to verify and further explore these procedures:

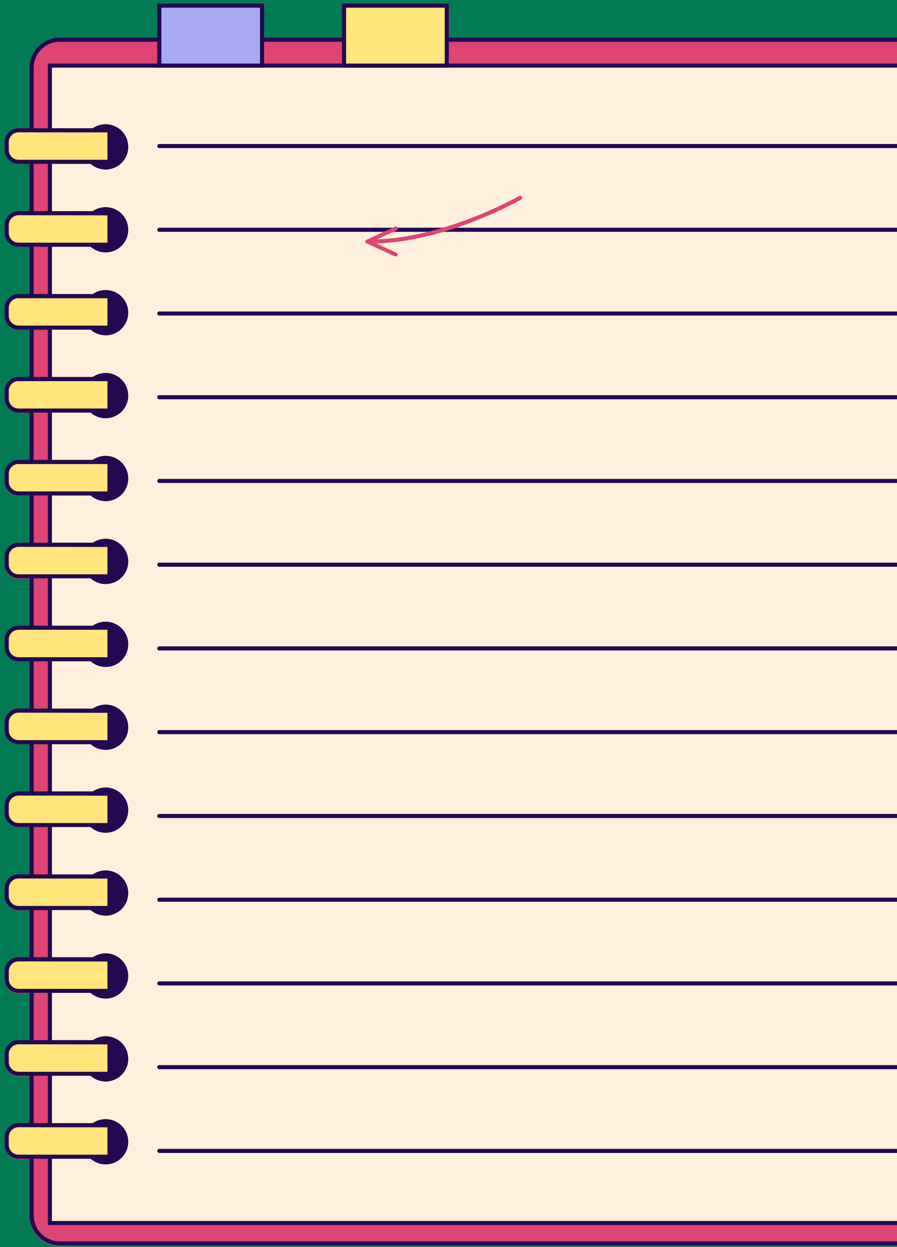
1. **Official Microsoft websites**
   - Microsoft Support for Windows Updates
   - Microsoft Support for Localize My Device
2. **Official Apple websites**
   - Apple Support for Updates on macOS
   - Apple Support for iOS Updates
   - Apple Support for "Find My Mac"
   - Apple Support for "Find My iPad"
3. **Official Android and Google sites**
   - Google Support for Android Updates

By following these steps, you can ensure that your devices are up to date and can be found if they are lost or stolen. This ensures the security of your personal and professional information, which is essential for home care workers.

MODULE 1 - CHOOSING YOUR DEVICE
AND PROTECTING IT

CHAPTER 4

MAKE YOUR DEVICES LAST: GOOD PRACTICES



Skills
to
Connect