MODULE 6

DIGITAL TAYO

Digital Foundations

Meta | Digital Tayo

Check-In

In our Zoom chat, type out your answer to the question:

How many characters is your longest password used in social media?

House Rules

Kindly change your name to:

ORG_NAME
(e.g. AHA! BD_Juan Dela Cruz).

Always show respect. This is a safe space.

Unmute only when you are speaking.

Press Zoom's Raise Hand button if you want to speak. When called, kindly unmute yourself and answer.

Learning Objectives

Define privacy and understand how to create safe spaces for oneself and others online.

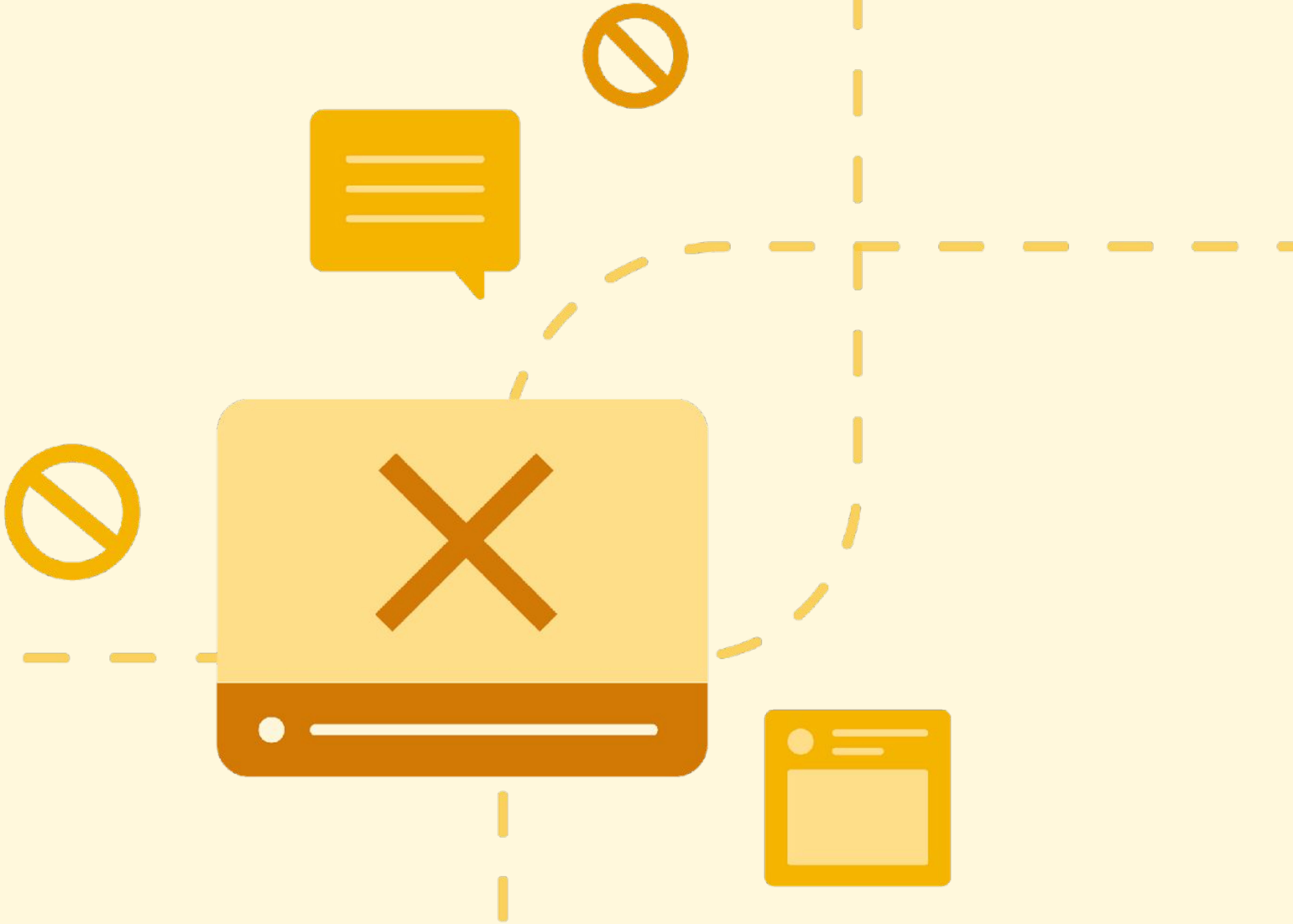
Identify how to keep their online information more secure by using and maintaining strong passwords.

Recognize the benefits and risks of public Wi-Fi networks and make informed decisions about when to connect to and use unsecured Wi-Fi.

Describe the risks of being online, develop strategies to engage in safer behaviors, identify spam messages and explain who should ask for their password.

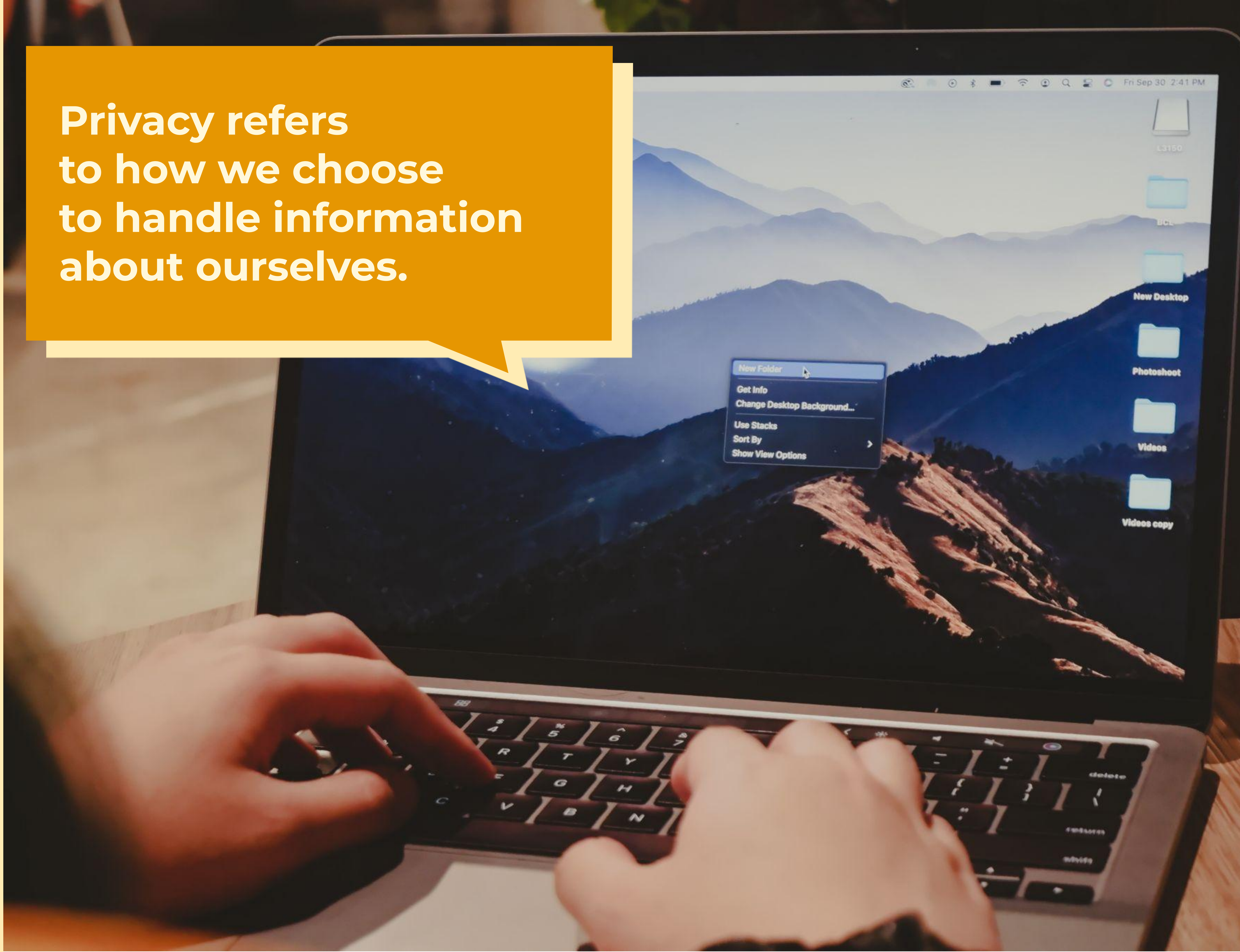
LESSON 1

Privacy and You



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

What is privacy?



Privacy refers to how we choose to handle information about ourselves.

Would you share where you live with...

Your parents/guardians or family members?

Your friends?

Your teacher or your boss?

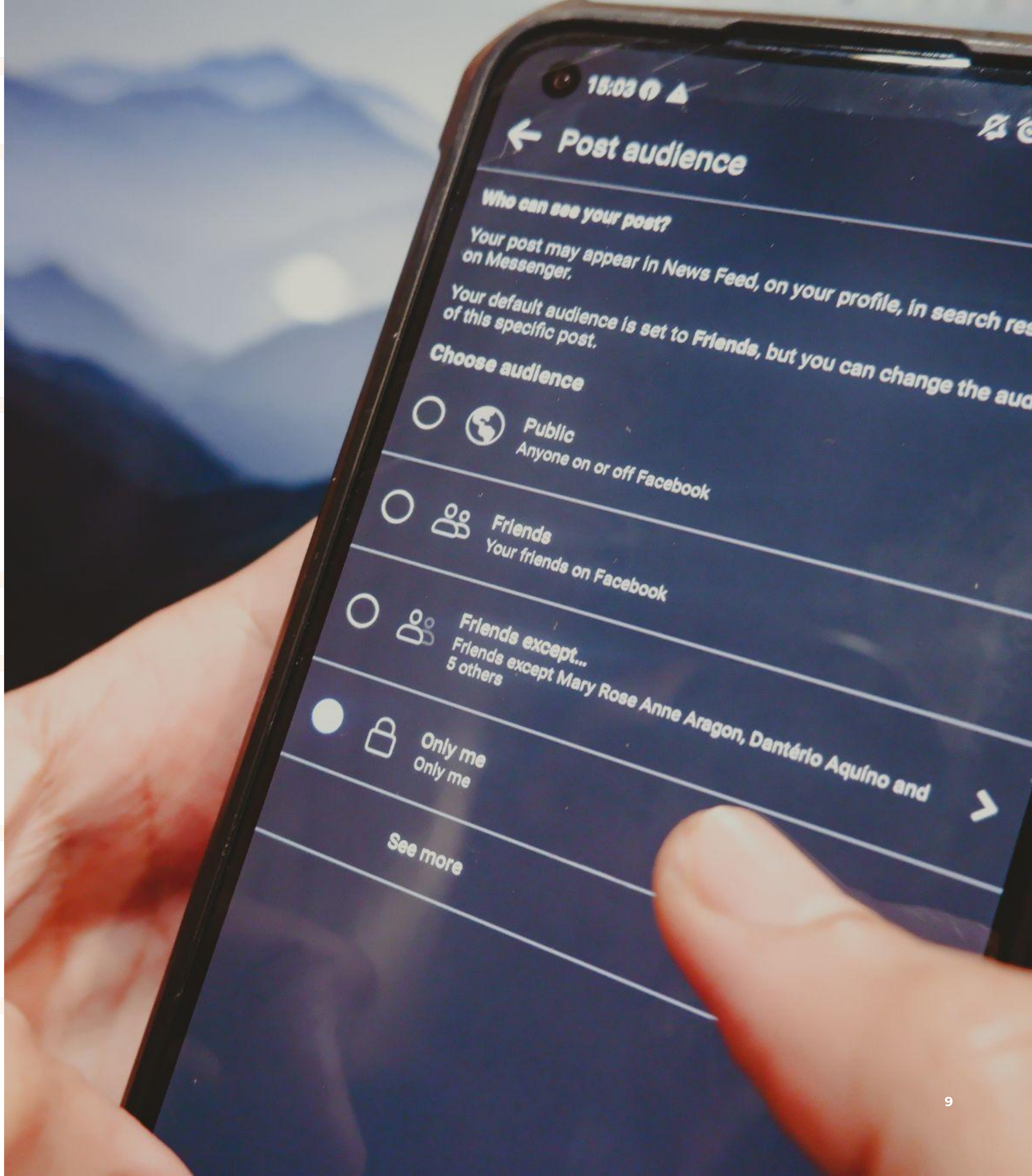
A stranger/person you don't know well?

A friend of a friend?

An organization or company?

How to control your privacy and manage your online reputation

Do you know your current privacy settings on every social media platform?



18:03

Post audience

Who can see your post?

Your post may appear in News Feed, on your profile, in search res
on Messenger.

Your default audience is set to Friends, but you can change the auc
of this specific post.

Choose audience

○ Public
Anyone on or off Facebook

○ Friends
Your friends on Facebook

○ Friends except...
Friends except Mary Rose Anne Aragon, Dantério Aquino and
5 others

● Only me
Only me

See more

Activity

- Is your overall account set to public, private, or something else?
- How did you decide on this setting?
- Are your current privacy settings what you want them to be?

Activity

Scenario

#1

Carla is 25 years old and has been working for the company she interned for 5 years. She wants to start looking for a new job next month. She loves computers and wants to get a job in the IT sector.

However, she doesn't know what jobs are available to her. She is aware that employers will want to see a CV, but she doesn't know how to write an effective one.

She would like to meet people with similar plans to get advice and recommendations on how to go about the process.

- **What type of social media platform would you recommend for Carla?**
- **What do you think would be the ideal privacy settings for that platform to enable her to achieve her goal?**
- **Please explain why.**

Activity

Scenario #2

Missy is 32 years old and is a full time mom. She has a daughter named Charlie.

She loves dancing. In her free time, she watches dance videos and practices the steps. She thought of teaching dance to little kids during the weekend.

- **What type of platform would you recommend?**
- **What do you think would be the ideal privacy settings for that platform?**

- **Please explain why.**

Activity

Scenario #3

Roy is 45 years old, and he is passionate about cooking and creating new recipes.

He has worked on several seafood dishes that he is very excited about, and he would love to share them with his friends and other people interested in cooking.

- **What type of platform would you recommend?**
- **What do you think would be the ideal privacy settings for that platform?**

- **Please explain why.**

Summary:

Privacy and you

Privacy refers to how we choose to handle information about ourselves.

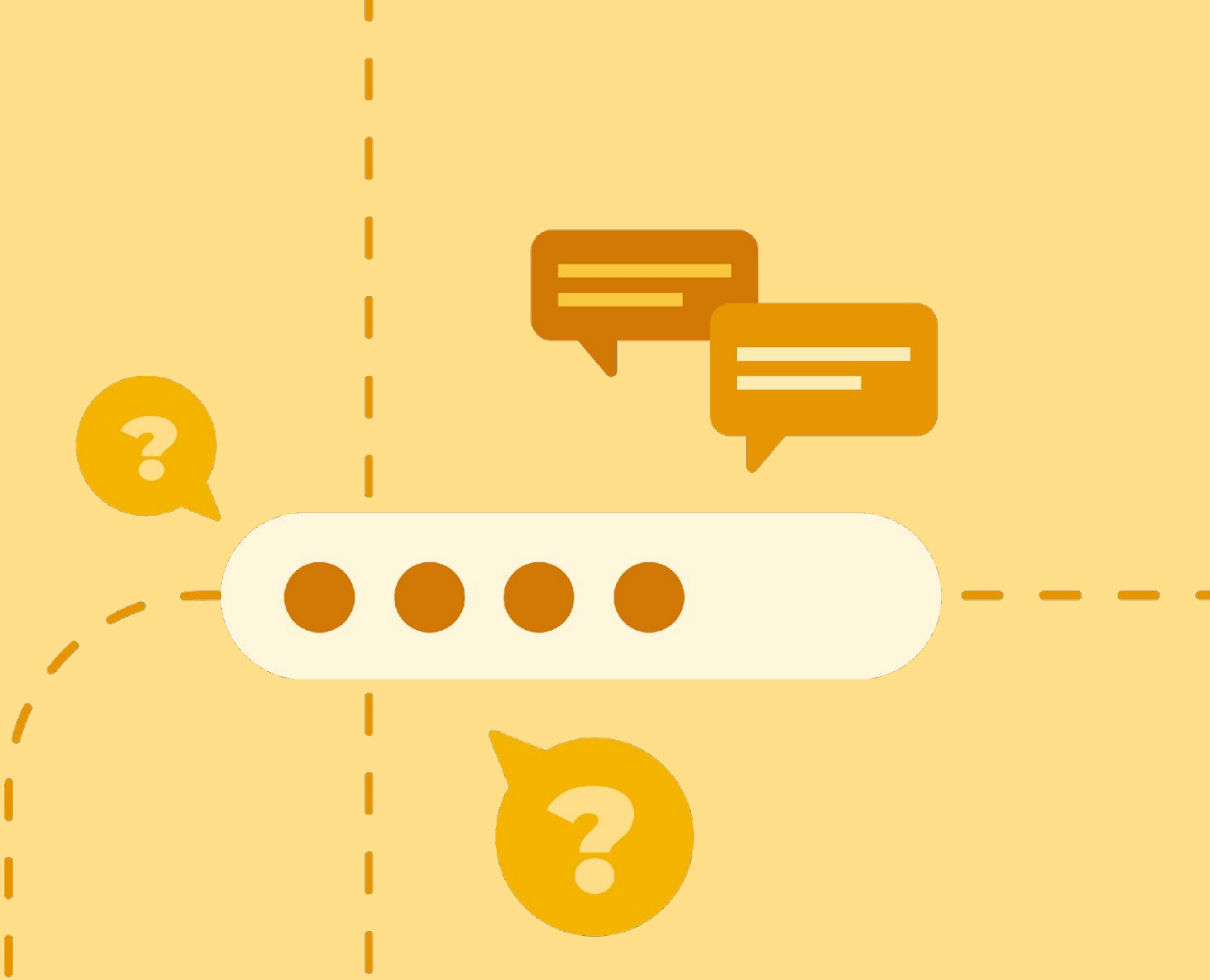
It is the ability to control what other people know about you.

Privacy is based on your own decisions.

It also changes depending on the type of information being shared and with whom it is being shared.

LESSON 2

Passwords



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

Let's talk about passwords!

Reminder: It is important not to share your actual passwords during this or any other exercises.

Passwords

What is a **Strong Password?**

What is a **Weak Password?**

Let’s check some passwords.

Which of the following are considered strong passwords?

D00R8377

A@-2&L4D~*’z>ux

i7ovemydog!!

Let’s check some passwords.

Which of the following are considered strong passwords?

D00R8377

A@-2&L4D~*’z>ux

i7ovemydog!!

How to create a Strong Password: A Password Recipe

- Include at least one number.
- Include at least one symbol.
- Include at least one uppercase and one lowercase letter.
- Passwords should be at least 7 characters.
- Passwords should be easy to remember (unless using a password manager).
- A password manager is a website/app that helps users save and organize their passwords.
- Passwords should not be a single common word or personal information (birth date, parent’s name, etc.).
- Passwords should not be shared between websites.

Examples:
Password Recipe

- C@ts-and-Dogs-Living-together
- jelly22fi$h
- d0gsaremybestfr13nds
- $m3llycat

How to create a Strong Password: Password Length

Connect a string of four or more unrelated words that makes it harder to guess.

26cheese + horse + train + table! = 26cheesehorsetraintable!

Activity

Create a Password Using: Password Length

Connect a string of four or more unrelated words that makes it harder to guess.

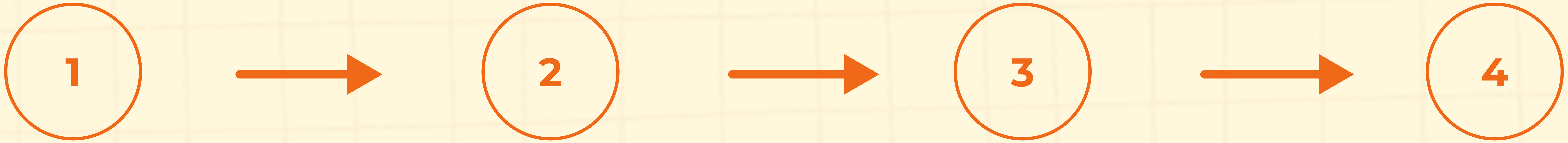
26cheese + horse + train + table! = 26cheesehorsetraintable!

Other ways your password can be weak

- Reusing a password for multiple accounts
- Using the same password for many years
- Using a password that contains personal information
- Forgetting your password

Multi-Factor (or Two-Factor) Authentication

How to use Two-Factor Authentication on Facebook



1 Go to your **Security and Login Settings** by clicking in the top-right corner of Facebook and clicking **Settings > Security and Login.**

2 Scroll down to **Use two-factor authentication** and click **Edit.**

3 Choose the authentication method you want to add and follow the on-screen instructions.

4 Click **Enable** once you've selected and turned on an authentication method.

How to use Two-Factor Authentication on Instagram

1. Tap 👤 or your profile picture in the bottom right to go to your profile.
2. Tap ☰ in the top right, then tap **Settings**.
3. Tap **Security,** then tap **Two-Factor Authentication**.
4. Tap **Get Started** at the bottom.
5. Choose **the security method you want to add** and follow the on-screen instructions.

How to Use Two-Factor Authentication on WhatsApp

1. Open **WhatsApp Settings.**
2. Tap **Account > Two-step verification > Enable.**
3. Enter a six-digit PIN of your choice and confirm it.
4. Provide an email address you can access or tap **Skip if you don't want to add an email address.**

   Note: Adding an email address is recommended as this allows you to reset two-step verification and helps safeguard your account.
5. Tap **Next.**
6. Confirm the email address and tap **Save** or **Done.**

Sharing passwords:

Do you share your passwords with other people?

Are there ever times when it's okay to share a password?

Do you share your passwords with anyone?

If you are close friends with someone, would them saying "If you care about me..." act as a motivator to share your password with them?

Activity

Learning About Passwords

1 What three insights from this session will you apply next time you have to create a password?

2 What is one instance where you feel that it is okay to share your password with someone else?

3 What are three strategies you can use to safely share your password with someone else?

4 What are three examples of what might go wrong if a password gets into the wrong hands?

Summary:

Passwords

Strong passwords help protect your information.

There are two approaches to creating strong passwords – follow a “password recipe” which includes harder-to-guess elements or rely on password length which uses a string of four or more unrelated words.

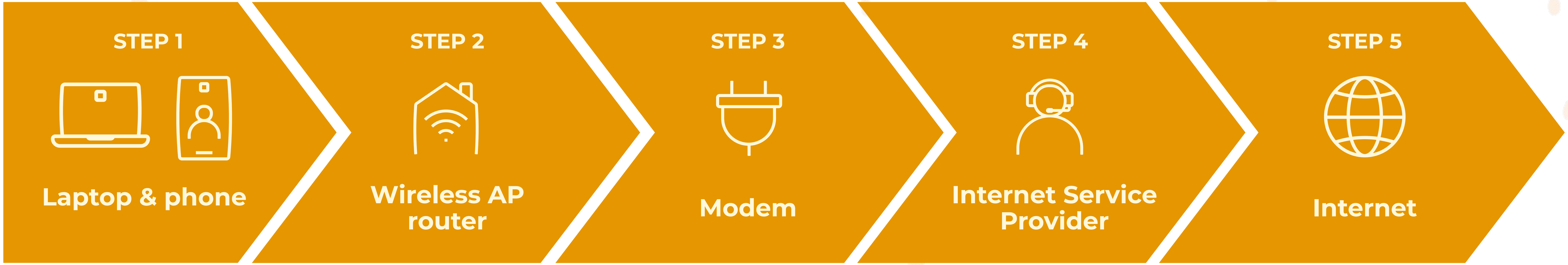
Two-Factor Authorization is an extra layer of security for your account to ensure you are the only person who can access it, even if someone else knows your password.

LESSON 3

Security Measures for Public Wi-Fi, Phishing and Spam

Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

How to Connect to the Internet



STEP 1

Laptop & phone

STEP 2

Wireless AP router

STEP 3

Modem

STEP 4

Internet Service Provider

STEP 5

Internet

Are all wi-fi networks safe?

Security Tools

HTTPS is a standard used by websites to encrypt data passed over the internet.

You should only enter sensitive information (e.g., passwords, credit card information) on web pages with the HTTPS:// prefix.

Connecting to Wi-Fi

What should you think about when connecting to any new network?

- Who owns the Wi-Fi network?
- Do you know these people personally?
- Do you trust these people?

You should only connect to a Wi-Fi network hosted by someone you know and trust!

When you are using the internet, you may expose yourself to risks through the mere act of accessing a web page, communicating online, or downloading data.

UBLIC WI-FI

What are these?

ILOVEYOU

MYDOOM

ZEUS TROJAN

CRYPTOLOCKER

EMOTET TROJAN

What is malware?

Malware is a harmful code that runs on your computer.

- Some malware can collect data from your computer.
- It can also allow hackers to take control of your computer.

What can you do to protect yourself against malware, spying, or tracking?

Be careful when clicking links, ads, or social media posts.

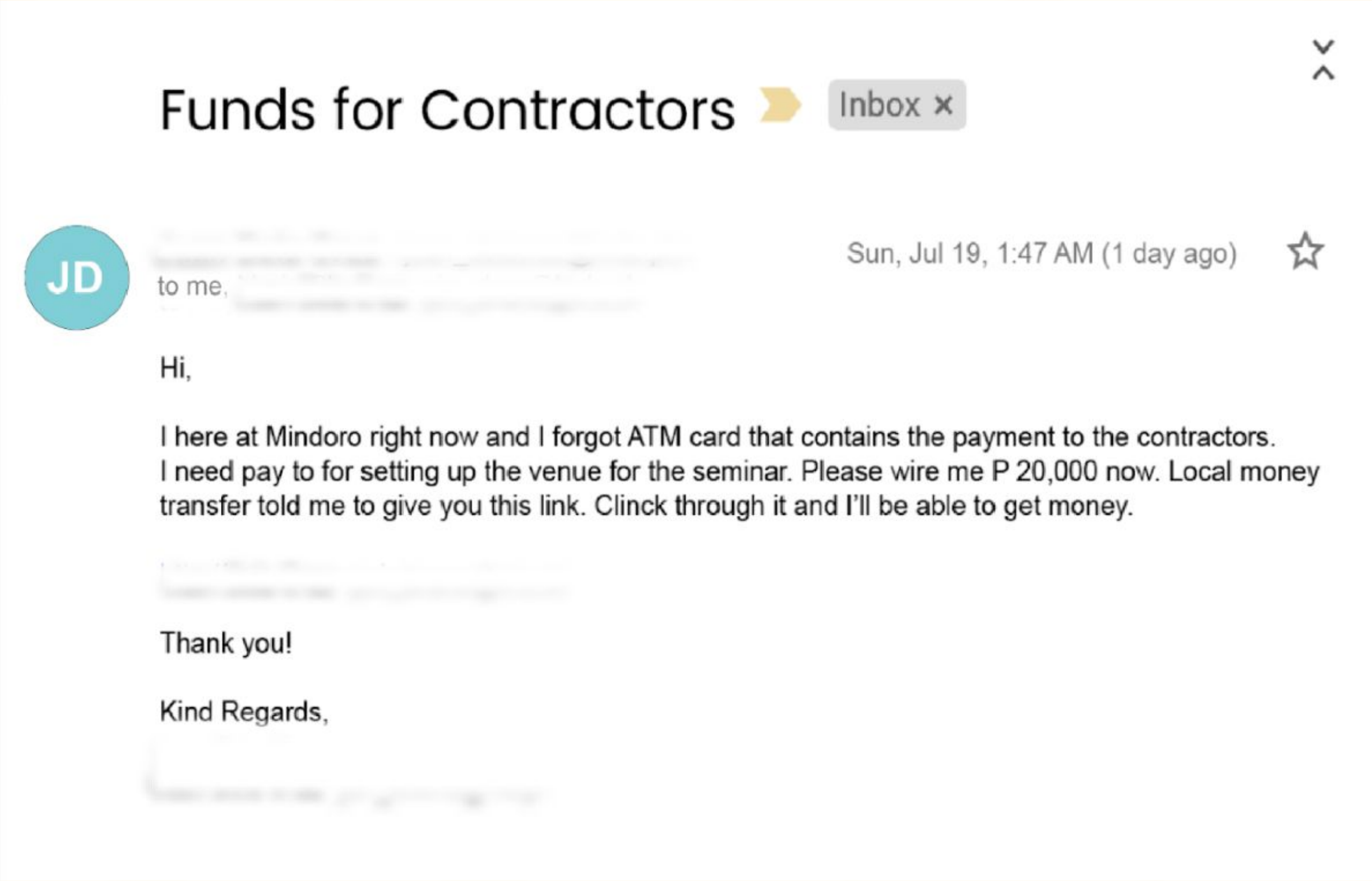
Only download or install software from trusted sources and be thoughtful about when you download executables (.exe, .pkg, .sh, .dll, or .dmg extensions).

You can use anti-virus software to prevent you from running malware.

You may also consider browser extensions that can, for instance, block plug-ins that make it harder for websites to track you.

Websites with the HTTPS:// prefix is secure because of a Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

A good rule is that SSL/TLS should protect any login page for an important account (like Google, Facebook, Twitter, or bank accounts). SSL/TLS makes it very hard for a hacker on the same network to send you a fake website.



Funds for Contractors

[redacted]
to me, [redacted]

Sun, Jul 19, 1:47 AM (1 day ago)

Hi,

I here at Mindoro right now and I forgot ATM card that contains the payment to the contractors. I need pay to for setting up the venue for the seminar. Please wire me P 20,000 now. Local money transfer told me to give you this link. Clinck through it and I'll be able to get money.

[redacted]

Thank you!

Kind Regards,

[redacted]

What do you think is wrong with this email?

Phishing

Phishing occurs over email from a scammer pretending to be a legitimate party.

What actions could you take to prevent yourself from accidentally downloading files that are harmful to your computer?

Activity

How might you identify spam?

Activity

Recognizing Connection Safety

What can you do to protect yourself against malware, spying, or tracking?

What actions could you take to prevent yourself from accidentally downloading files that are harmful to your computer?

What risks might be associated with sharing your password?

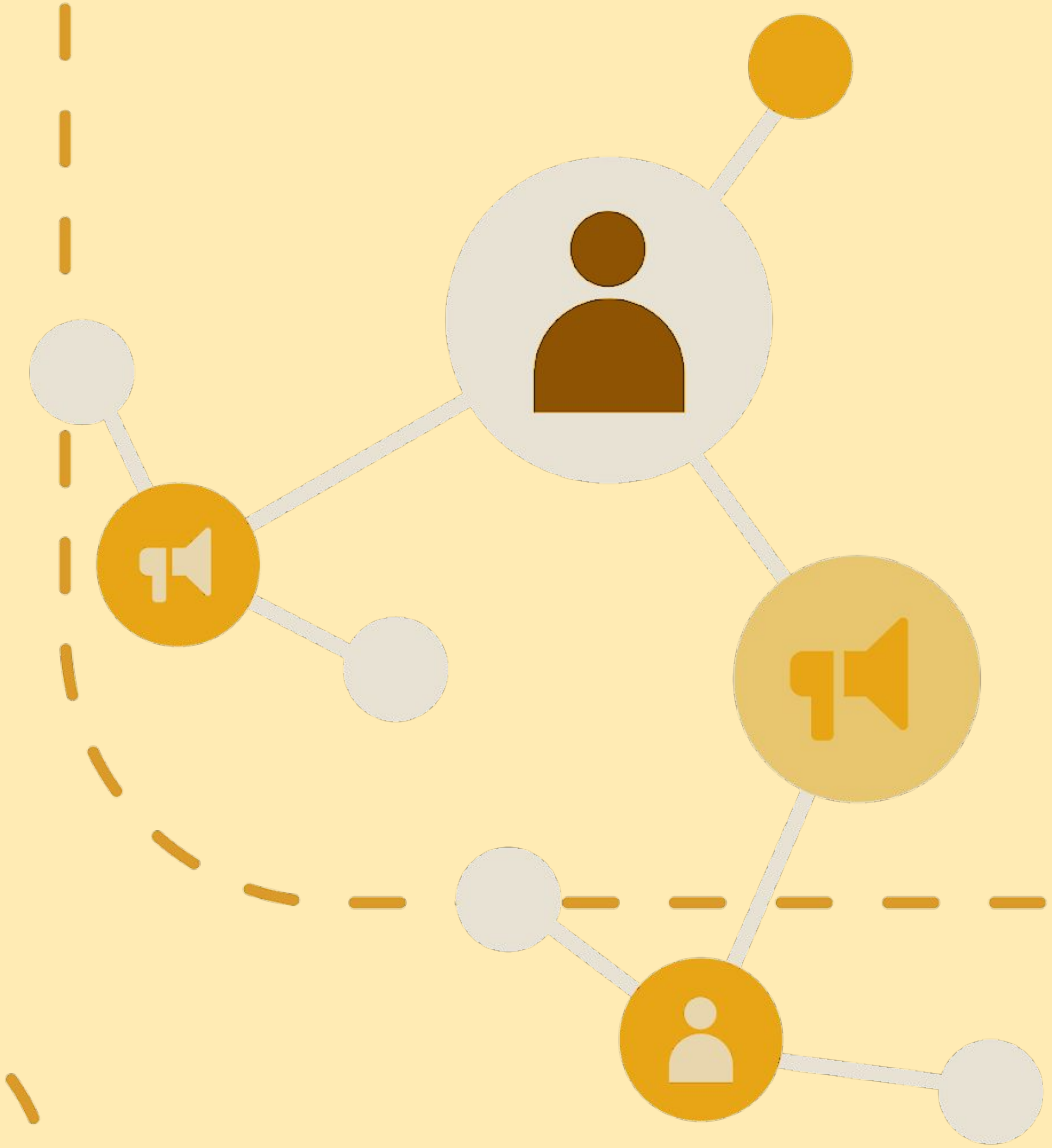
Summary:
Security Measures

There are serious risks if you connect to the wrong network.

Be careful when clicking links, ads, or social media posts.

The act of “phishing” primarily occurs over email from a scammer pretending to be a legitimate party.

Wrap-up



Key points

Privacy refers to how we choose to **handle information about ourselves**.

Privacy also changes depending on the **type of information being shared** and **with whom it is being shared**.

Strong passwords help **protect your information**.

Key points

Two-Factor Authorization is an **extra layer of security** for your account to **ensure that you are the only person who can access it**, even if someone else knows your password.

There are two approaches to creating strong passwords – follow a **"password recipe"** which includes **harder-to-guess elements** or **rely on password length** which uses a string of four or more unrelated words.

There are **serious risks** if you **connect to the wrong network**.

Key points

Encryption was created to **make it more difficult for hackers** to see what you are sending.

Be **careful when clicking** links, ads, or social media posts.

The act of "**phishing**" primarily occurs over **email from a scammer** pretending to be a legitimate party.

What are your Top 3 KEY TAKEAWAYS?

Share them with 3 people after this.

MODULE 6

DIGITAL TAYO

Digital Foundations

Meta | Digital Tayo