MODULE 2

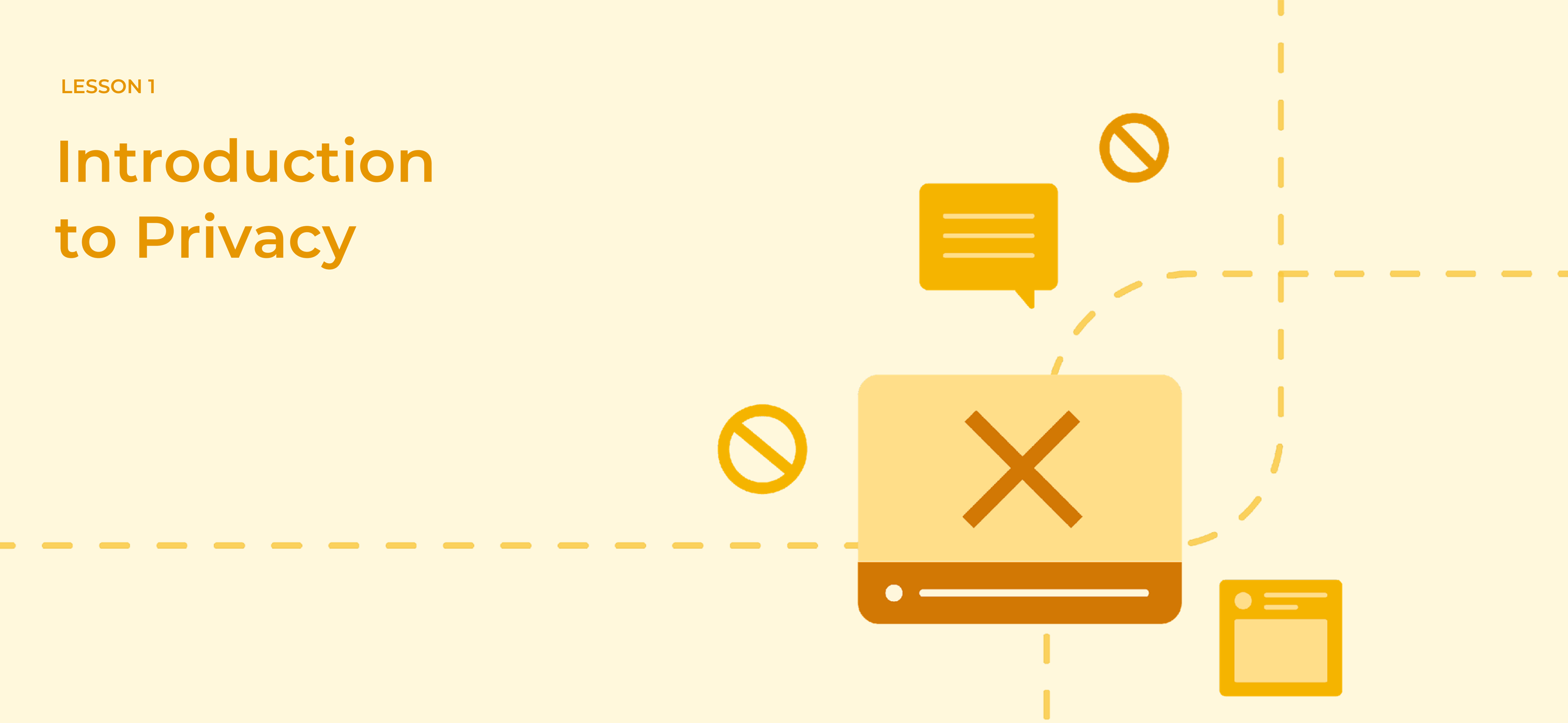
WE THINK DIGITAL

Digital Foundations

Meta | We Think Digital

LESSON 1

Introduction to Privacy



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.

Activity

The Privacy Game

What Does Privacy Mean to You?

What Is Privacy?

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

It’s important that we become aware of our own understanding of privacy and that we think about whether we’re comfortable with that understanding or not.

Are there some other things that aren't necessarily secrets that you might still want to keep private from people you don't know well/people you've just met?

Are there some things you might keep from your parents/guardians or your friends?

Did you learn anything about your personal understanding of privacy that surprised you?

Are there some things you might keep from your teachers or other educators?

Activity

Your Personal Understanding of Privacy

Task 1

Find three examples online where someone shared or posted something that you would personally keep private.

Task 2

For each example, write a paragraph description of why you would choose to keep this information private.

Task 3

Explain if or how your personal opinion on sharing this information changes depending on the context.

LESSON 2

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.

Activity

The Guessing Game

- Were there any pieces of information that you did not share with anyone? Which ones? Why?
- Did everyone make the same choices about what to share? Why/why not?
- Depending on whom you share with, why might you share more, or less, of this kind of information? When would you share it?

Activity

The Guessing Game

- How easy was it to connect each piece of information to the person who wrote/said it?
- Were there instances where a given response might have inadvertently conveyed something beyond the actual response?
- What assumptions do you think other people might make about you if you shared the information you wrote down as part of the Guessing Game with the wider world?

Would You Share Where You Live With...

Your parents/guardians or other important adults in your family?

Your friends?

Your teacher?

A stranger/person you don't know well?

A friend of a friend?

An organization or company?

COMMUNICATING IN TEXT MESSAGES:

Is It Different From Communicating It in Person?

How to Control Your Privacy and Manage Your Online Reputation

Do You Know What Your Current Privacy Settings Are on Each Social Media Platform?

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

- When does it make sense to have public sharing and when might private settings be preferable?
- Do you feel comfortable sharing your information with the social media platforms you use or the companies advertising on these platforms?
- Does this conversation make you think differently about your privacy settings?

Activity

Scenario

#1

Akari is 13 years old and she loves singing.

She feels that she is not that great at it yet, but she would like to share her passion with her friends and get their input on it. She is considering adding some videos of her singing some of her favorite songs on a social media platform.

- 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

#2

Ren is 16 years old and he is passionate about cooking and creating new recipes.

He has worked on several chicken dishes that he is very excited about, and he would love to share the ingredients and how they are prepared 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. Also explain if or how your personal opinion on sharing this information changes depending on the context!

Activity

Scenario

#3

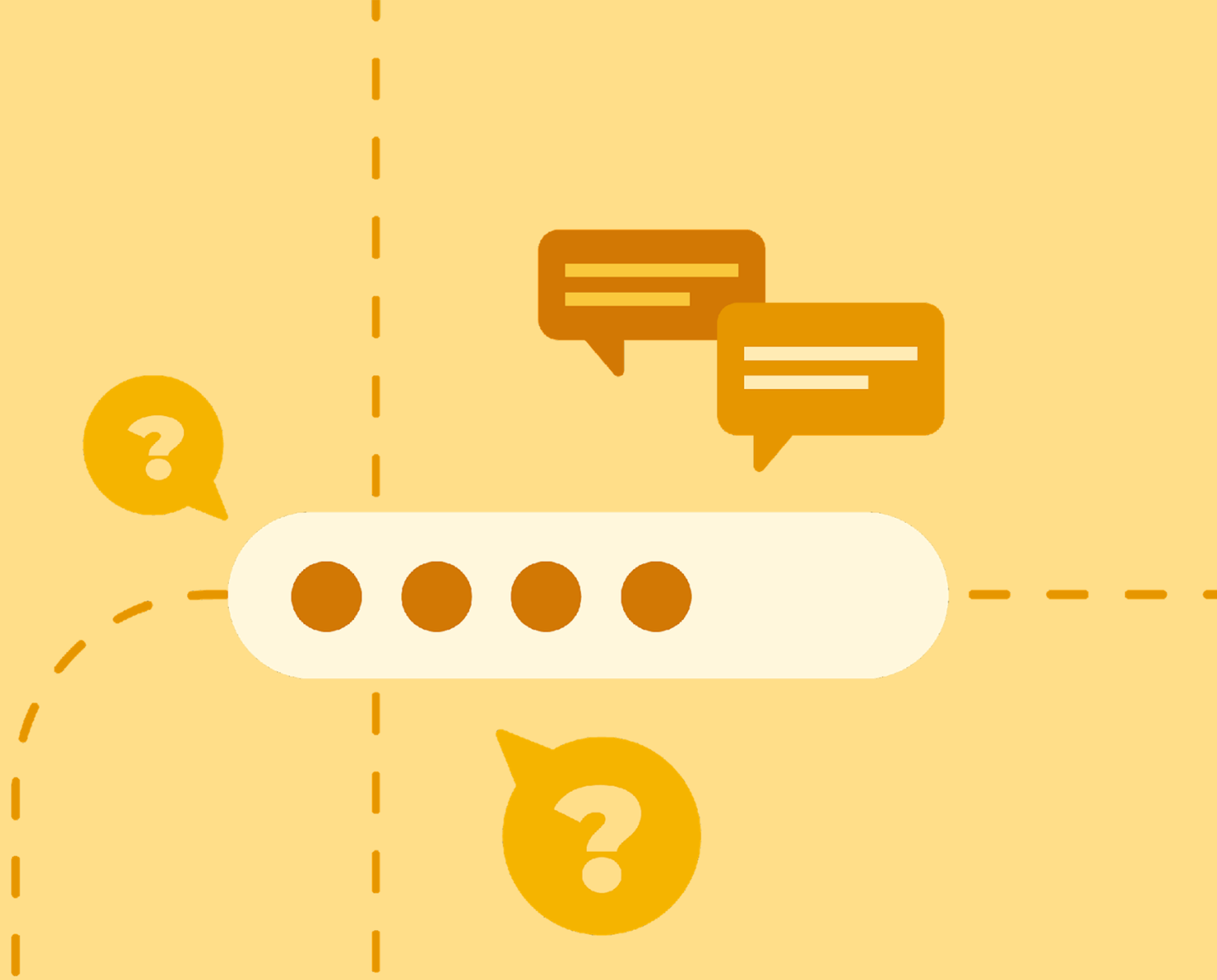
Yuna is 18 years old and wants to start looking for a job next month.

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 with people who have similar plans so she can get advice and recommendations on how to go about the process.

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

LESSON 3

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.

Class Interaction

What would happen if someone who wanted to cause trouble learned the password to your favorite social media platform?

What would happen if a hacker learned the password to your parent's/guardian's online banking account?

How Can a Hacker Learn a Private Password?

Passwords

What Is a Strong Password?

What Is a Weak Password?

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.

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 the “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.

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!

Multi-Factor (or Two-Factor) Authentication

Other Ways Your Password Can Be Weak

Reusing a password for multiple accounts

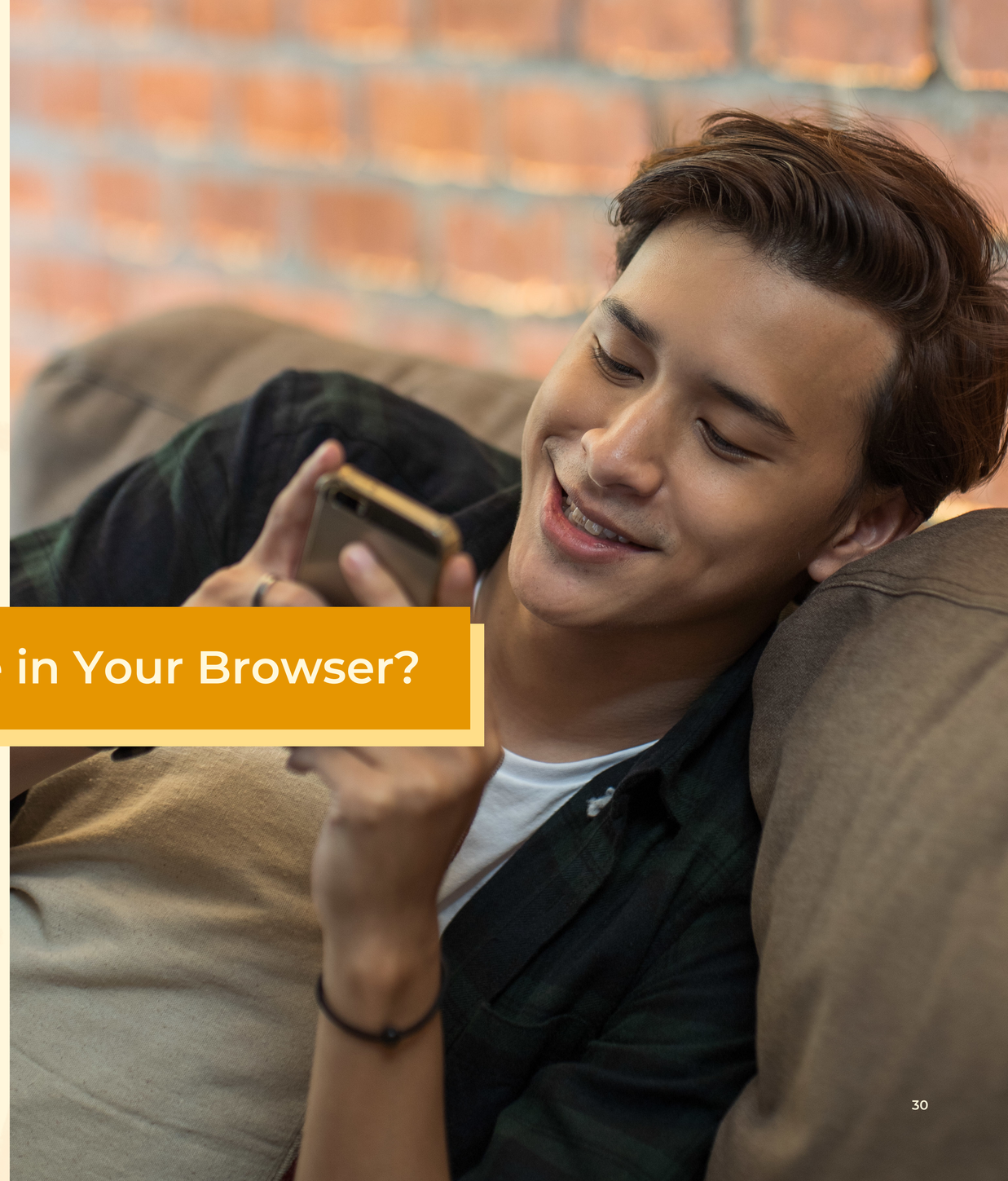
Using the same password for many years

Using a password that contains personal information

Forgetting your password

Do You Use a Password Manager?

Do You Use the “Save Password” Feature in Your Browser?



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?

Social Hacking/ Social Engineering

If someone knows enough personal information about you, they might be able to guess your password!

Activity

Learning About Passwords

1. What are three insights from this session you will apply the 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?

How to Use Two-Factor Authentication on Facebook

- Go to your Security and Login Settings by clicking in the top-right corner of Facebook and clicking **Settings** > **Security and Login**.
- Scroll down to **Use two-factor authentication** and click **Edit**.
- Choose the authentication method you want to add and follow the on-screen instructions.
- Click **Enable** once you've selected and turned on an authentication method.

How to Use Two-Factor Authentication on Instagram

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

How to Use Two-Factor Authentication on WhatsApp

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

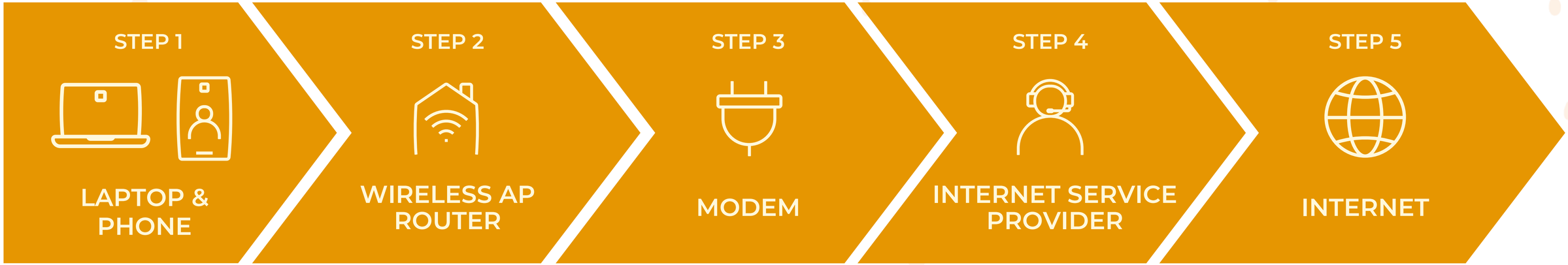
  Note: Adding an email address is recommended as this allows you to reset two-step verification and helps safeguard your account.
- Tap **Next.**
- Confirm the email address and tap **Save** or **Done.**

LESSON 4

Public Wi-Fi

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



How to Connect Your Laptop or Phone to the Internet

ACCESS POINT

An access point is anything that transmits (broadcasts) a Wi-Fi signal and provides access to the internet.

WIRELESS AP ROUTER

A router is a device that creates a network between all the devices in a given location.

MODEM

A modem is a device that creates and maintains a connection to your Internet Service Provider (ISP) to give you access to the internet.

Wi-Fi

What are the benefits of Wi-Fi?

What are some of the drawbacks of Wi-Fi?

Do you think there are any security concerns when using Wi-Fi versus a wired internet connection? Why?

Why is it that you lose Wi-Fi access on your phone as you leave a building?

Are All Wi-Fi Networks Safe?

The Three Common Encryption Protocols for Wi-Fi Networks

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access Version 2 (WPA2)

Encryption

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

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.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) are names for the technology that keeps HTTPS secure.

Security Tools

Browser security indicators will also communicate Extended Validation (EV) certificate information. EV certificates are given to websites that verify their identity to a certificate authority.

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!

Should You Use This on Your (Home/School/Coffee Shop) Wi-Fi Network?

Read Online News/Blogs

Send Your Credit Card Number

Check Your Personal Email

Connection Safety

Activity

Draw a Timeline of a Regular Day, Marking the Wi-Fi Networks to Which You Connect.

Can You Describe the Network?

Who Else Is Connected to It?

How Secure Is It?

What Are the Opportunities and Risks?

LESSON 5

Cybersecurity, 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.

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.

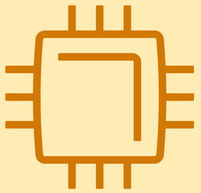
It is sometimes possible for websites you access, people on the same network, or even third parties to figure out your location or other information about you when you browse.

- Why might malicious hackers try to access your information online?

- Why would a website you are not logged into want to keep track of who you are?

- What information are people looking for?

- Does anyone know what malware is? What can it do?



What Is Malware?

Malware is 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.

Most malware is simpler, though, such as websites that imitate secure portals like a bank or extensions that put advertisements in your browser to make money.

Online Risks

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

Does the URL match what you expect?

Do you get to the same page when you type it again or search for the website?

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.

Security Tools

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 your computer from running malware.

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

Do You Know Whether You Are Secure When You Use the Internet?

What Actions Could You Take to Prevent Yourself From Accidentally Downloading Files That Are Harmful to Your Computer?

Sharing Passwords

Do You Think It’s Okay to Share Your Password?

What Risks Might Be Associated With Sharing Your Password?

Activity

Spam

How Might You Identify Spam?

MODULE 2

WE THINK DIGITAL

Digital Foundations

Meta | We Think Digital