Co-funded by
the European Union

DATA PRO

Protect Yourself Online: Privacy, Security, and Digital Best Practices

AdM
ArchiviodellaMemoria

What kind of information do you share online every day?

What kind of information do you share online every day?

- Name and surname
- Photo
- Position
- School
- Interests
- Posts, likes, comments…

Why is data so important?

Why is data so important?

Data is valuable. Why? Companies use data to:

Show personalized ads

Understand what we like to buy or look at

Sell our data to other companies (call centers)

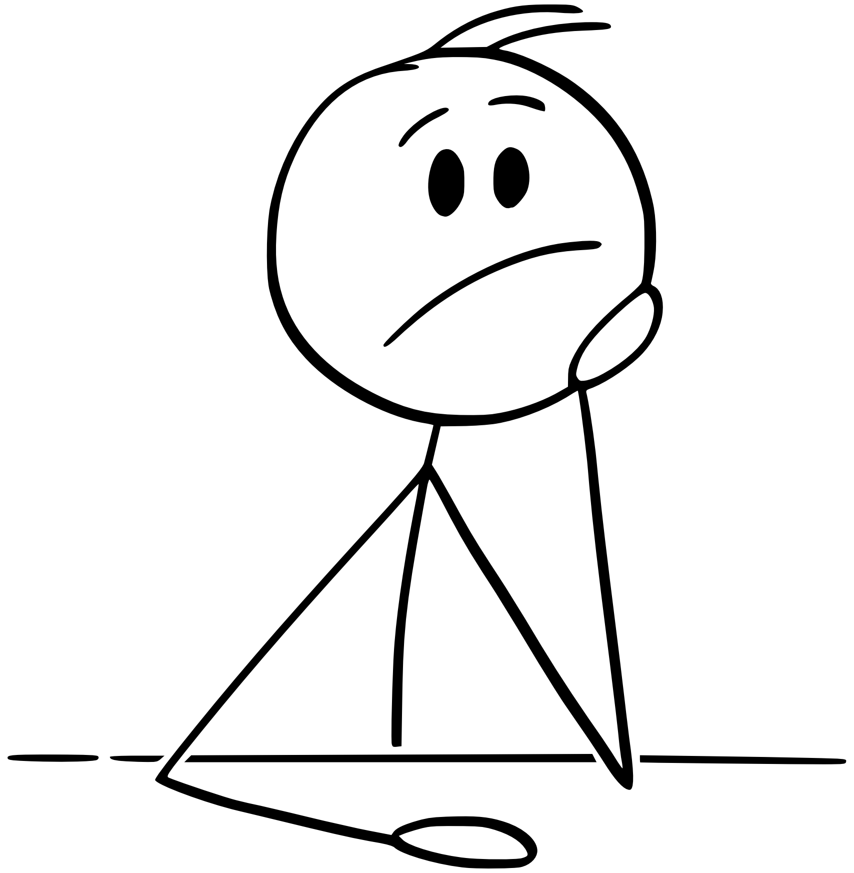
Every click, like, or search says something about us: age, tastes, habits, interests, even where we are!

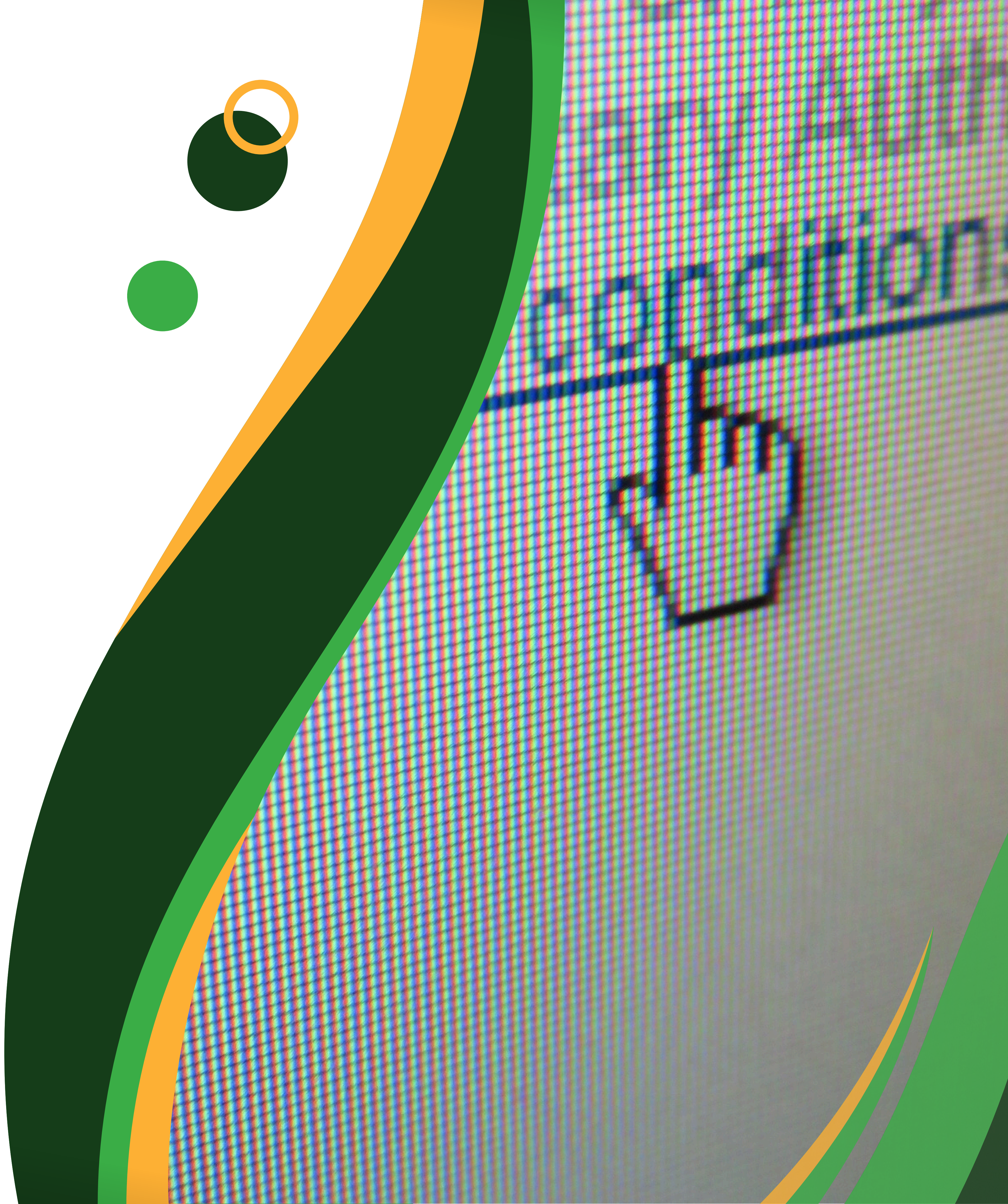
If an online service is “free,” the product is you... or rather, your data.

DATA PRO

Any information you share online can be seen, saved, or used by others, even without your consent.

How is your data collected?

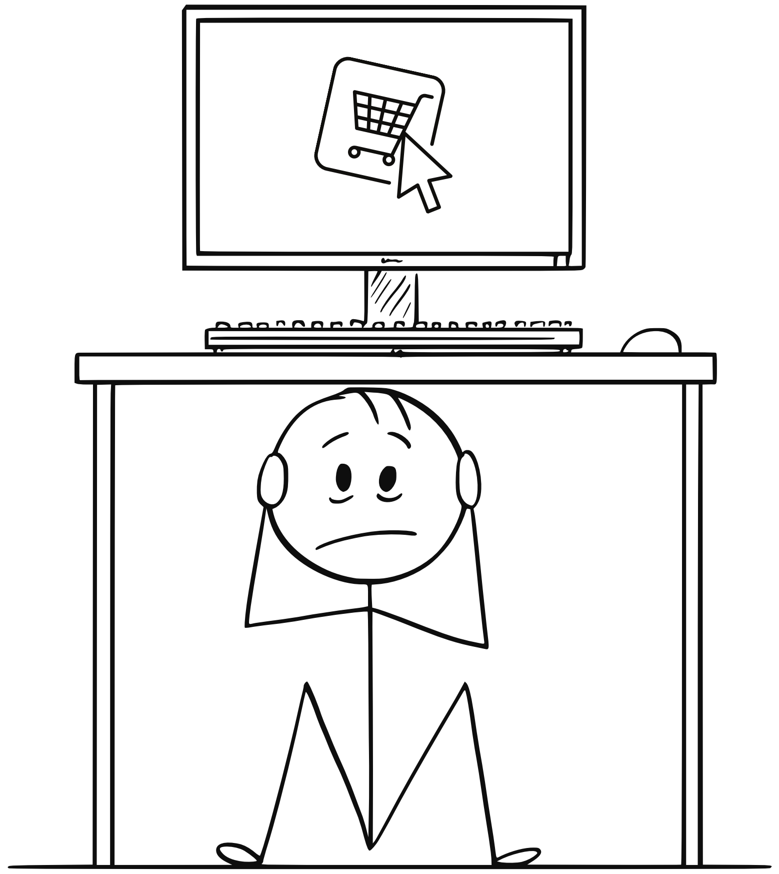


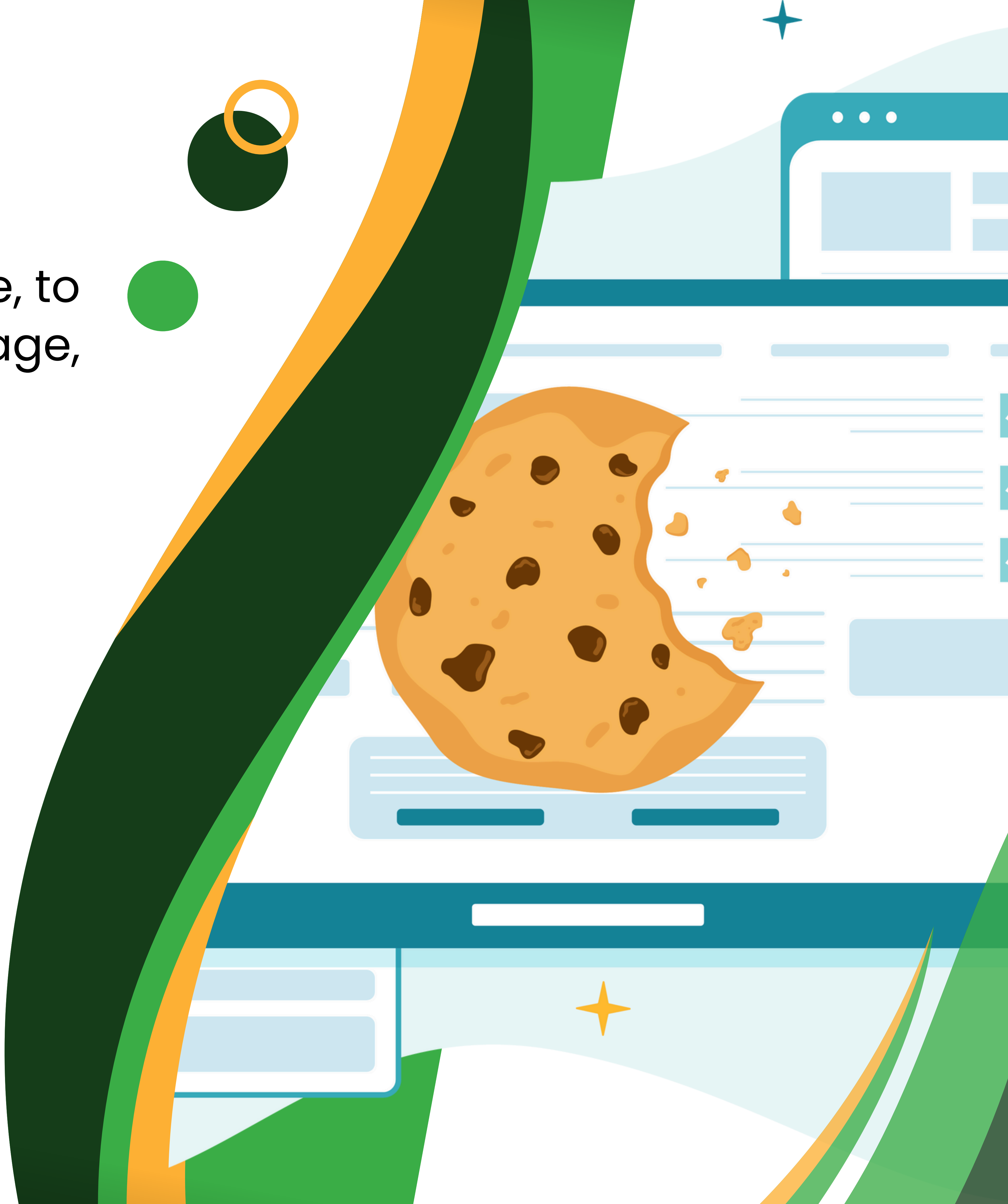


Cookies

Small files saved on your device by a website, to remember your preferences such as language, login, products in your cart, etc.

Have you ever had a website "remember" what you looked at?





Phishing

Attempts to trick you into providing personal or banking information.

It presents itself as:

- Suspicious emails
- SMS with strange links
- Fake login pages

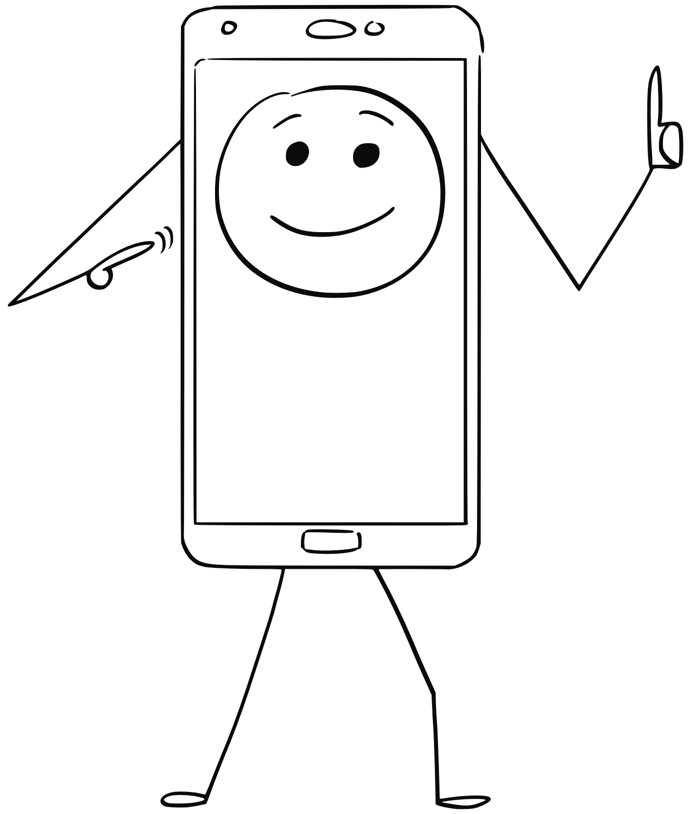
Have you ever received a suspicious message?

Secure data sharing

Share only necessary information online.

- Think before you post.
- Use privacy settings.

What information is best NOT to share?



DATA PRO

Secure connection

When you visit a website, the address you see at the top of your browser almost always begins with http:// or https://

- **HTTP stands for HyperText Transfer Protocol.** It's the "language" websites use to communicate with your browser. It's not secure: the data you send (like passwords or messages) can be intercepted by someone else.
- **HTTPS :the "S" at the end stands for Secure.** The data you send or receive from the site is encrypted (i.e., protected). No one can read or steal what you're typing.

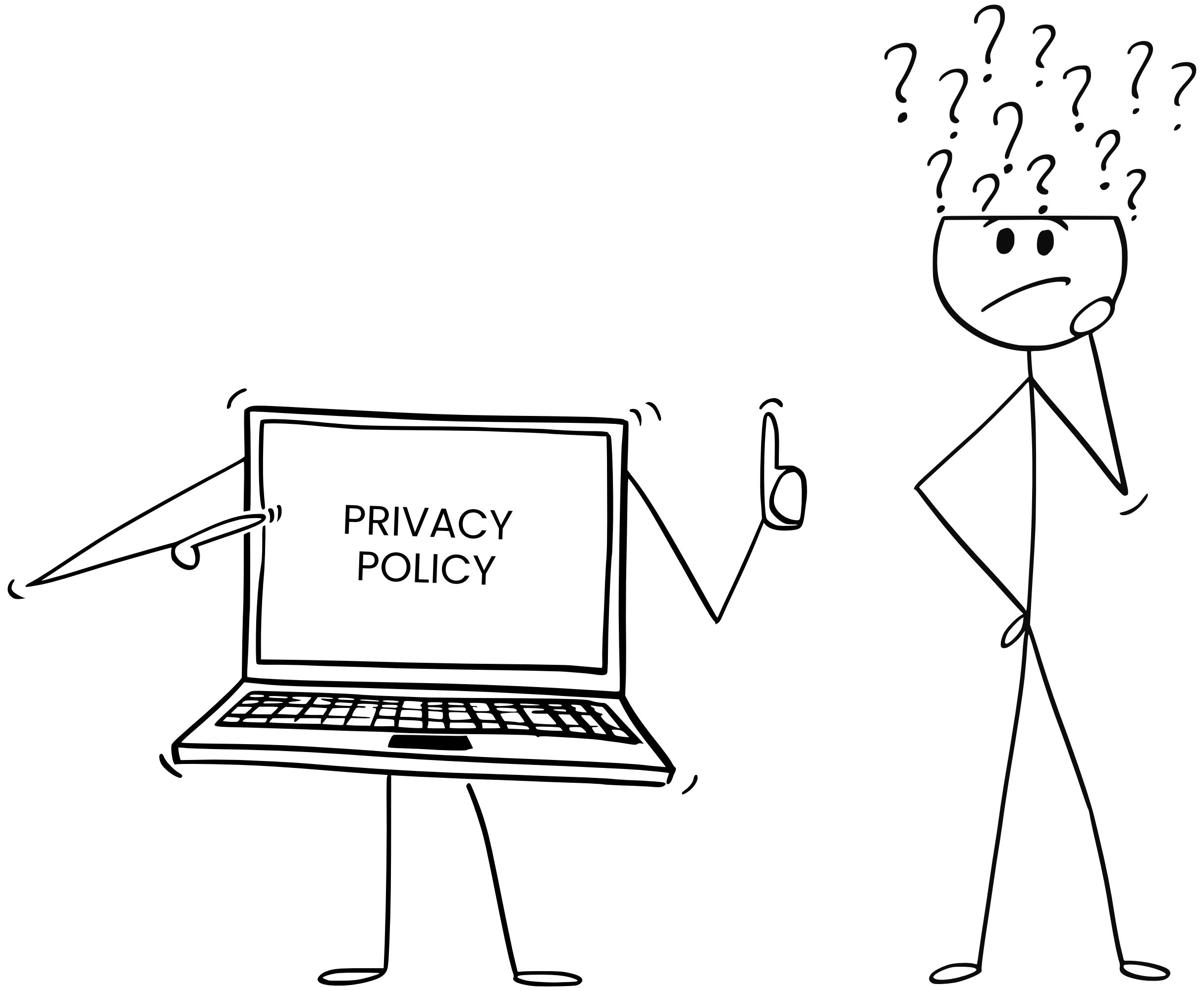
Privacy Policy

Documents that explain how a site collects, uses, and protects your data.

Reading them helps to:

- Know what we are accepting
- Understand who can access our data

Have any of you ever read a privacy policy?



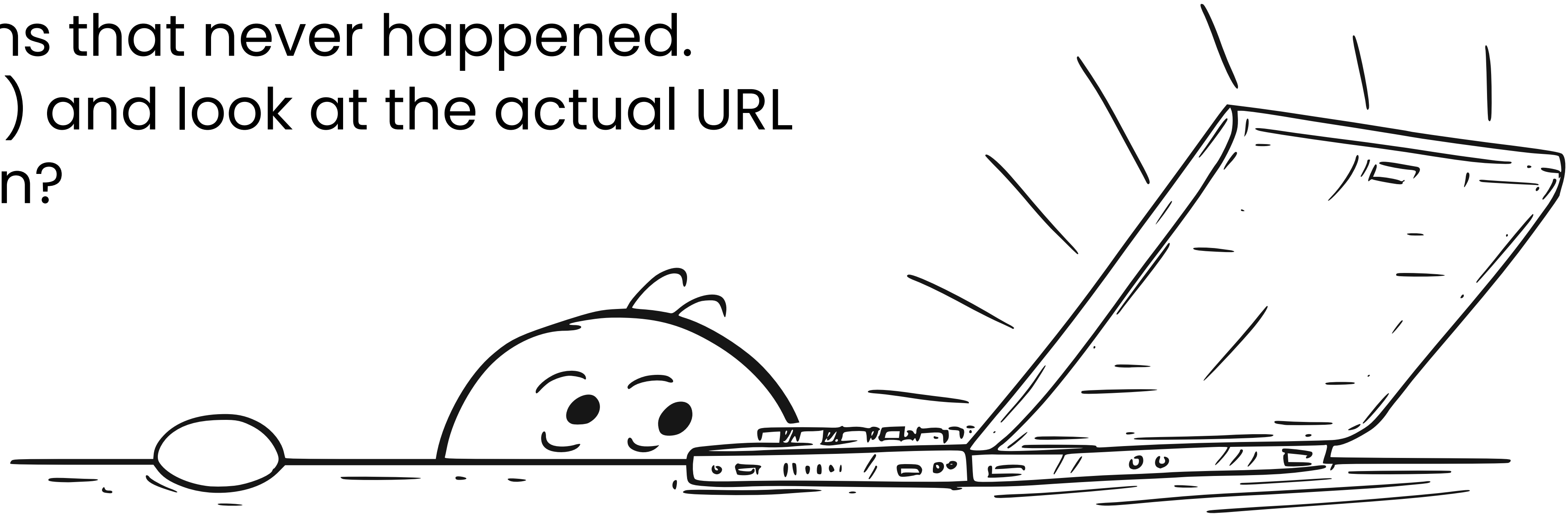
DATAPRO

Exercise “Recognize Phishing”

Phishing is when someone pretends to be a well-known company or service to steal your personal information (such as passwords, credit card numbers, etc.).
They often send you emails or messages with strange links you have to click.

Red Flags – Warning Signs of Phishing

- Alarmist or urgent tone: “Immediate action required,” “Your account will be blocked,” “Only 24 hours!”
- Request for personal or banking information: no reliable service will ask you to enter passwords or card numbers via email.
- Suspicious or strange links: links may appear legitimate but lead to fake sites (e.g., netflix-support.com instead of netflix.com).
- Unofficial senders: emails from unofficial or generic addresses (e.g., customers_netflix123@gmail.com)
- Grammatical errors: messages often contain poorly translated sentences or obvious errors.
- Offers too good to be true: prizes or contest wins that never happened.
- Fake URLs: hover over the link (without clicking!) and look at the actual URL at the bottom. Is it different from the one shown?



Exercise “Recognize Phishing”

1. Divide into small groups.
Each group receives a series of emails or SMS messages (real or fake).
2. Read each message carefully.
Your job is to figure out whether it's a real message or a phishing attempt.
3. For each message, look for suspicious clues together.
- Alarmist or urgent tone (e.g., “Immediate action required!”)
- Request for personal data (password, card number, etc.)
- Suspicious or strange links (with strange names or too many hyphens)
- Strange or unreliable sender
- Grammatical errors or strange Italian
- Offers too good to be true

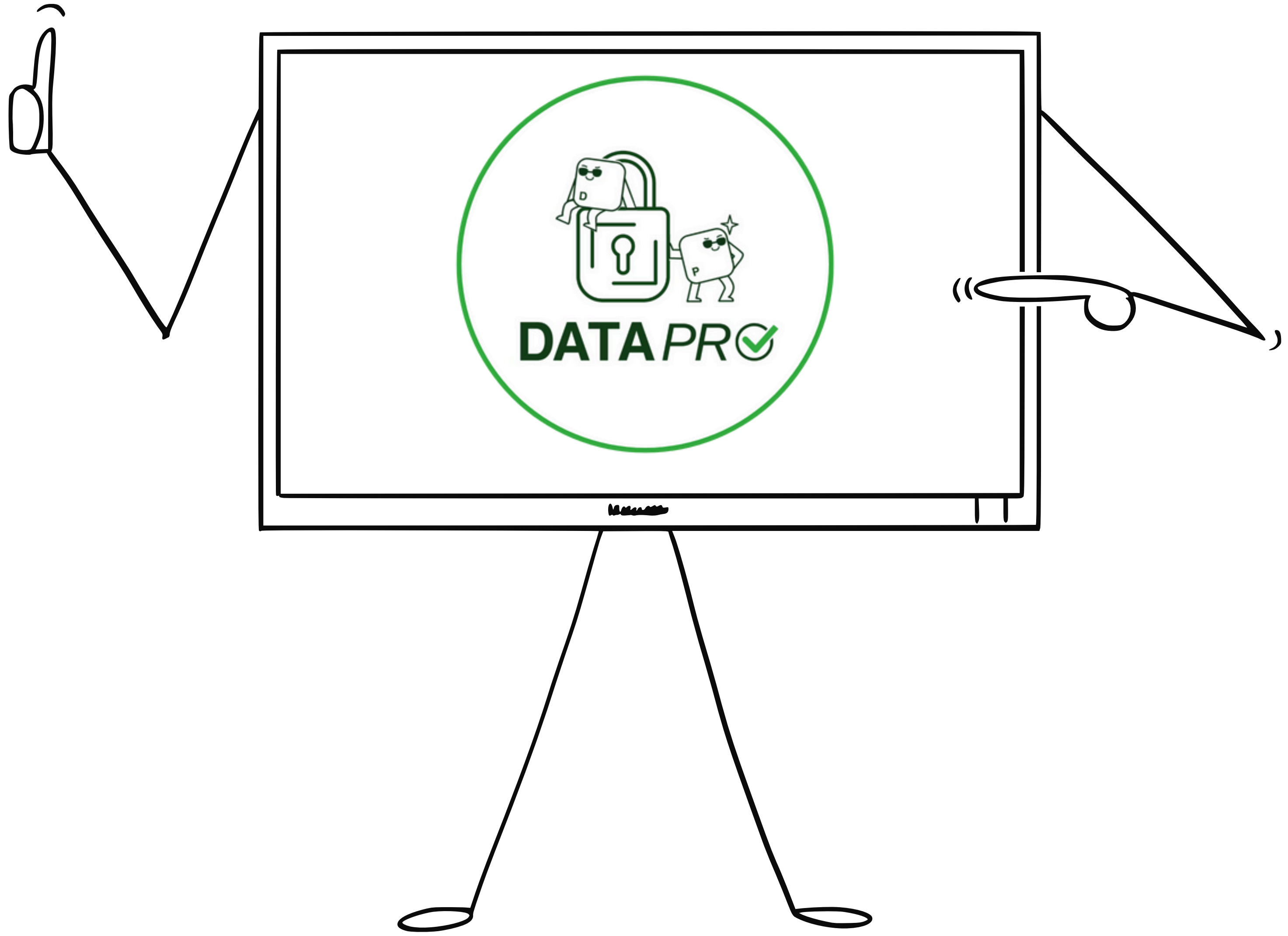
Note or underline any items that seem strange or dangerous to you.

DATAPRO

Exercise “Recognize Phishing”

4. Open the Erasmus+ DataPro project chatbot website: https://www.datapro.education/students/
5. Copy suspicious messages into the chatbot.

The chatbot will tell you if it's phishing and explain why.



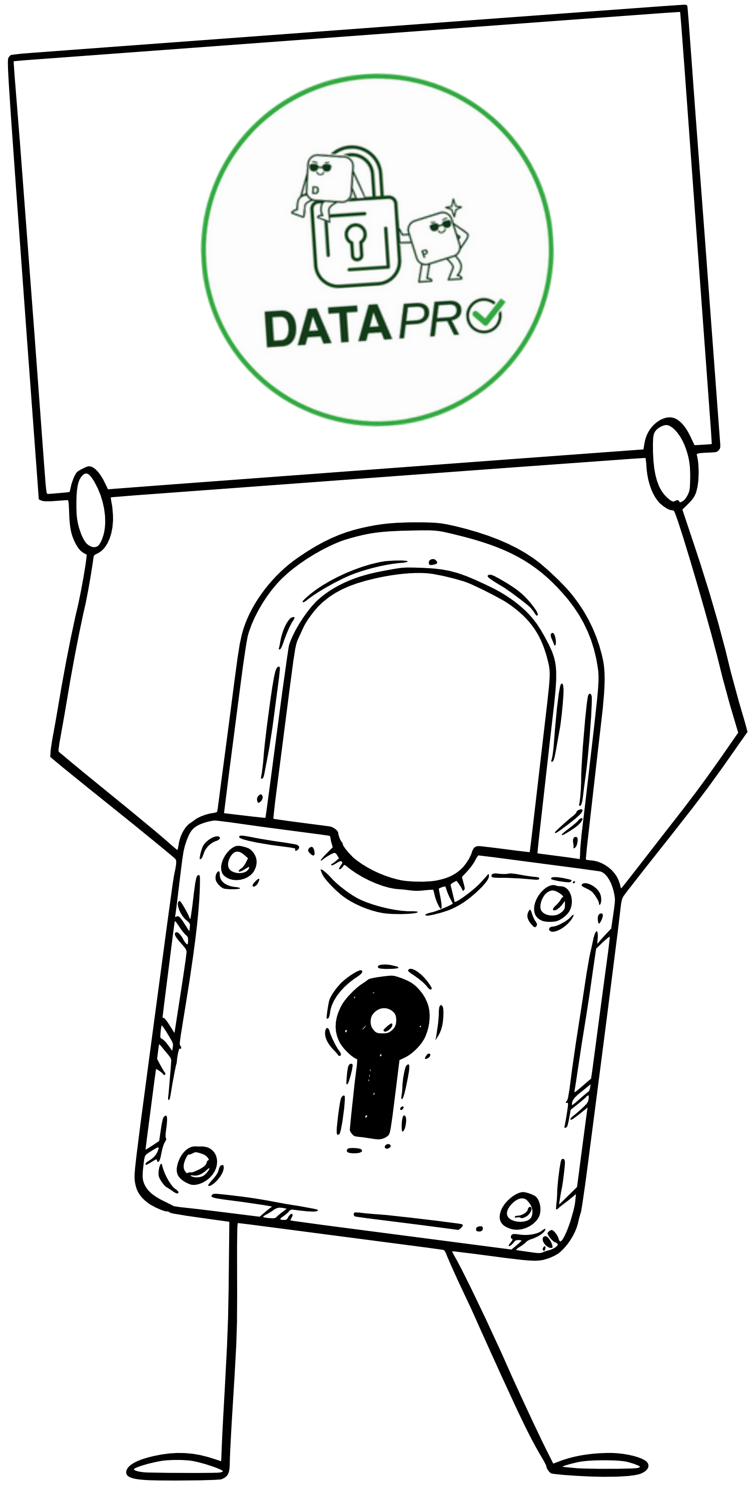
Exercise “Secure Content Sharing”

Sharing online means making information potentially accessible to everyone, often permanently: “Any content we publish – a photo, a comment, a piece of personal data – can be saved, shared, manipulated or used without our control.”

1. Divide into pairs or small groups.
2. Each group will have a specific scenario to discuss.
3. Read the scenario together and answer the following questions. You can get help from the Datapro Chatbot:

- What is potentially problematic about this situation?
- What risks are involved?
- How could we act more safely?

4. Each group must reflect on how to deal with the situation
5. Describe and share with the class.



Co-funded by
the European Union

DATA PRO

Thank you

Visit Our Website
Datapro.education

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.