EUROPEAN CYBERSECURITY MONTH

IS SOMEONE **PHISHING** FOR YOUR INFORMATION?

It starts with...

- an email
- a text message
- a direct message on social media
- a phone call

which seems to be coming from...

- the government
- your telecom, electricity or gas provider
- your bank
- another organisation or person you are in touch with regularly

requesting you to...

- send your personal information, such as your bank details, username of accounts, identification number
- make a payment
- open a link or an attachment

How to protect yourself against phishing attempts?

Learn to spot a suspicious message, call or email!

1. Check the sender's number or email address.
2. Look at how the email or message is phrased and if there are any spelling or grammar mistakes.
3. Check at what time the email or message was sent.
4. Analyse the tone of the message. Is there a sense of urgency, excitement, anxiety?
5. Check the list of recipients of the email or message. Are these familiar to you? Is it a long list of recipients?

You have been phished! Now what?

- Change the passwords of your affected account(s); use a unique password for every account.
- Change the usernames of your accounts, if possible.
- Check regularly for unusual activities taking place on your accounts.
- Report the incident to relevant authorities and organisations to help prevent the fraudulent use of your data.
- Share your experience with friends and family to help them stay safe.

10th EUROPEAN CYBER SECURITY MONTH anniversary

Cyber First Aid MAP

edps.europa.eu