Digital Literacy by SPCO

Part 3

2025

Email Phishing

Online Security Course

What you'll learn by complete this 7 part course :

Part 1:
What is Online Security?
Part 2:
Creating Strong & Safe Passwords
Part 3:
Spotting Phishing & Fake Emails
Part 4:
Secure Browsing Habits
Part 5:
Protecting your Devices
Part 6:
Public Internet & Safe Internet Use

Why email phishing matters?

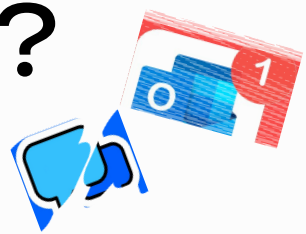
Phishing is when someone pretends to be a trusted company or person to trick you into giving them personal info — like your **password**, **bank details**, or **security codes**.

These scams often come by:

- Email
- Text messages (SMS)
- Fake websites

Knowing what to **look for** can keep you safe.

What does it look like?



Phishing emails try to create **urgency** or **fear** so you'll act fast and not think.

Common red flags:

🚩 Says: "Your account will be closed!"

🚩 Asks for personal or payment info

🚩 Spelling or grammar mistakes

🚩 Strange-looking email address (e.g. support@amazzon.co)

🚩 Links that lead to **suspicious websites**

Fake Email Example:

“Hello, your paypal account has been suspended due to suspicious activity.

Please log in immediately to verify your account: [Click Login Link]”

What’s wrong?

- Urgent language
- Fake login link
- Likely a phishing attempt to steal your paypal login.

How to check if an email is real

Check Sender's Email

Real: support@paypal.com

Fake: support@pay-pal.help.biz

Don't click suspicious links

Hover over the link (don't click!) and look at where it's going.

When in doubt don't respond.

Go to the official website yourself

Open a new tab and type in the company's website manually.

Take Action

Open your email inbox and:

Find **1 email** that looks suspicious or “off”

Look for **3 red flags** (spelling, sender, links, urgency)

If it’s phishing, **mark it as spam or report it**

Tip: No real company will **ever ask you for your password nor credit card numbers** by email.

Next Lesson

Browse the internet safely