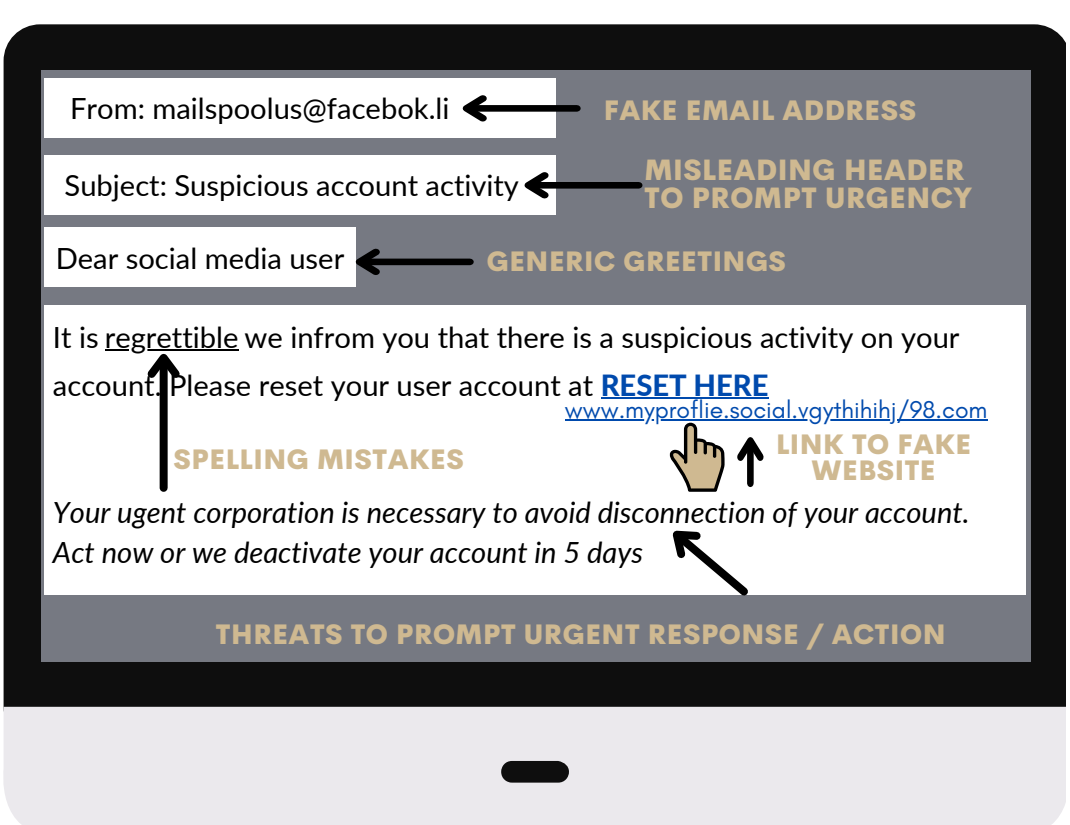
CYBERSECURITY

Identifying Phishing Attacks

Phishing attacks often appear as fraudulent information from seemingly reputable sources by email. The aim of phishing is to get sensitive information or install malware.

HOW TO RECOGNIZE PHISHING ATTACKS

Phishing attacks come in many forms. One common example is through emails. These are sent from hackers who use **fake email addresses** and send **viruses as attachments** or include **fake websites** embedded in the body of the email.



HELPFUL TIPS TO AVOID PHISHING

VERIFICATION OF FAKE WEBSITES

A simple one-letter omission of a website can take users to a fake website that steals your information.

It is good practice to verify the URL address on the address bar of the web browser before entering personal information.

Clicking attachments | Updating passwords | Social Media Requests | Using a New Wi-Fi Network

REPORT PHISHING ATTACKS

Forward phishing emails to the Anti-Phishing Working Group **reportphishing@apwg.org**

Forward phishing text messages to **SPAM (7726)**

Report phishing attacks to the Federal Trade Commission (FTC) **reportfraud.ftc.gov**

References:

- Cisco. (n.d.). *What is phishing?*. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
- Terranova Security . (2022, July 17). 19 examples of common phishing emails and how to avoid them. https://terranovasecurity.com/top-examples-of-phishing-emails/

PURDUE UNIVERSITY | College of Education

Project TIME — Teaching Innovations in Multimodal Education, a GEER grant initiative of Learning Design & Technology