PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information.

Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual.

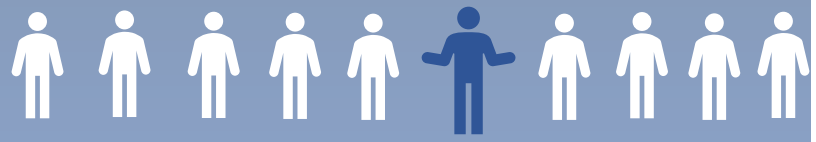
The email may also request personal information like account numbers, passwords, or National Insurance number click on a link, attackers use it to access their account(s).

Scammers are after your:

- **Passwords**
- **Financial info**
- **Money**
- **Identity**

WHY DO WE FALL FOR THESE SCAMS

- Urgency
- Desire to please
- Greed
- Curiosity
- Complacency
- Fear



PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS

1 OUT OF 10!

WATCH OUT FOR

- Spelling & Grammar Error
- Sender Address
- Things That Sound Too Good to be True

BEWARE OF

- Unsolicited messages
- Attachments
- Links
- Login Pages

IF YOU SEE SOMETHING SAY SOMETHING!

Report Phishing Emails to
itservicedesk@polfed.org

INFORMATION TECHNOLOGY
POLICE Federation

When in doubt, throw it out:

Links in emails and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the sender – it's best to contact them by phone, delete or, if appropriate, mark it as "junk email." Contact the IT Service Desk to be sure the email is not legitimate.

Think before you act:

Be wary of communications that implore you to act immediately, ask for personal information, or if they offer something that sounds too good to be true.

Use Stronger Authentication:

Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email. A stronger authentication helps verify a user has authorised access to an online account. Contact the Service Desk to get support in getting the Authenticator App.

Be wary of Hyperlinks:

Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.