# Email Phishing

**Objective –** Simulating an e-mail phishing attack.

Subject: Urgent: Verify Your Email Account to Avoid Disruption

Dear [Recipient],

We hope this message finds you well. Due to recent security upgrades, we require all users to verify their email accounts to ensure the continued safety and functionality of our system.

To complete the verification process, please click on the following link: [Malicious Link]

Note: Failure to verify your account within the next 24 hours will result in temporary suspension.

Thank you for your prompt attention to this matter.

Sincerely,

[xyz]

Phishing is a type of cyberattack that tries to trick you into giving away your personal or financial information by pretending to be someone or something you trust. Phishing emails or text messages may look like they come from a legitimate source, such as your bank, your online payment service, or your utility company, but they are actually sent by scammers who want to steal your personal identifiable information.

**How to avoid/catch possible phishing E-mail attacks?**

To avoid phishing, you need to be careful and vigilant when you receive any email or text message that asks you to click on a link, open an attachment, or provide any sensitive information. Here are some tips to help you differentiate and avoid phishing emails:

- Check the sender's email address. Sometimes, scammers use spoofed or similar-looking email addresses to trick you into thinking they are someone else. For example, an email from your bank might come from support@yourbank.com, but a phishing email might come from support@yourbank.net or support@your-bank.com. If you notice any inconsistencies or typos in the email address, be suspicious.
- Look for spelling and grammar errors. Scammers often use poor language or automated translation tools to create phishing emails. If you see any obvious mistakes or awkward phrases in the email, it could be a sign of phishing.
- Beware of urgent or threatening messages. Scammers often try to create a sense of urgency or fear in their phishing emails, such as saying that your account is on hold, that you need to verify your information, or that you have won a prize. They want you to act quickly and impulsively, without thinking too much. Don't fall for their tricks. Always take your time and verify the authenticity of the message before you respond or click on anything.
- Don't click on suspicious links or attachments. Scammers often use links or attachments to direct you to fake websites or to infect your device with malware. These links or attachments may look legitimate, but they could lead you to phishing sites that ask you to enter your information or download malicious software. To check if a link is safe, hover your mouse over it and look at the URL that appears. If it doesn't match the sender's domain or the expected destination, don't click on it. Similarly, don't open any attachments that you are not expecting or that have unusual file names or extensions.
- Don't provide personal or financial information via email or text message. Legitimate companies or organizations will never ask you to send them your passwords, account numbers, or Social Security numbers via email or text message. If you receive such a request, it is likely a phishing attempt. If you are not sure, contact the sender directly using a trusted phone number or website, and never use the contact information provided in the email or text message.

- Use spam filters and antivirus software. Spam filters can help you block or flag unwanted or suspicious emails, while antivirus software can help you detect and remove malware from your device. Make sure you keep your spam filters and antivirus software updated and enabled at all times.

Report phishing emails or text messages. If you receive a phishing email or text message, don't delete it. Instead, report it to your email provider, your company's IT department, or the Federal Trade Commission (FTC) at ReportFraud.ftc.gov. You can also forward phishing emails to spam@uce.gov or phishing text messages to SPAM (7726). Reporting phishing can help stop scammers from targeting you and others in the future.