What is Phishing?

Phishing occurs when attackers send convincing emails or messages to trick recipients into downloading malicious software or clicking harmful links. Often these messages are disguised as a trusted source, such as the organization you work for or your bank.

How to identify a phishing attempt

- Message that calls for an urgent action or threats
- Misspellings and bad grammar
- Mismatched email domains
- Suspicious looking links or unexpected attachments
- Request for sensitive information

How to protect yourself

- Train employees how to spot and report phishing attempt
- Do not engage with the sender or the contents of the email. Delete it and/or report it to your organization's IT department.
- Utilize multi-factor authentication solutions
- Utilize email filters
- Deploy and maintain anti-virus software.

Resources

https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

https://www.ncsc.gov.uk/guidance/phishing