Phishing

Phishing is a social engineering method most frequently used by cyber criminals to capture personal and/or financial information. It uses email with faked information and takes the user to dangerous websites. Phishing emails are able to fake the sending address and reproduce logos of legitimate senders such as a bank or a government agency.

A phishing email usually has a few common elements:

- It claims to come from a credible organisation
- It claims to come from someone familiar
- A tone of urgency that asks the recipient to take immediate action
- A threat of negative consequences, or the promise of some kind a reward

The goal is to trick a user into divulging personal and/or financial data such as credit card numbers, account user names and passwords or other valuable information. In some situations, the phishing email may trick a user into downloading dangerous malware onto their computer.

More Than One Way to Phish

Phishing used to only include mass emails that targeted thousands of people with a fake message. As time has gone on the methods have grown more advanced and are harder to recognise.

- **Spear Phishing** is the targeted version of phishing with attacks that are customized to the recipient of the email (corporate executives, for example). They are unique and usually contain personal information about the target or their work and is directly addressed.
- **SMS Phishing** or Smishing uses cell phone or smartphone text messages to phish. The method sometimes includes a phone number directly to a scammer who will try to trick you. Be wary of quizzes or questions that prompt you to respond because they can secretly subscribe you to premium services at a cost per text.
- **Vishing** scams make use of Voice over Internet Protocol (VoIP) which allows people to talk over their computer lines (e.g. Skype or FaceTime). The criminals call and leave an automated message saying the person's credit card or bank account has been compromised, depleted or closed, and to call a phone number for information. When people call the number, they are asked to provide their personal information.

Have you been spammed or Phished?

Many people have received phishing emails asking for their username and password and have responded to these requests. The responses were used to compromise that person's mailbox and send thousands of spam emails to other users. If you believe you have been compromised, secure your account and report it.

How do you guard against Phishing?

Remember that legitimate businesses, financial institutions, and help desks should never ask you for personal or confidential information via email, voice or text message. Be ware of unexpected messages and verify them by contacting . Less sophisticated messages may set off alarm bells because there are misspelled words or faulty grammar. **You can 'hover' your mouse over a URL to see if it is identical to what is written; if they are different, this is an indicator that the source is probably not legitimate.**

In general

- Be careful if the email was unsolicited.
- Be suspicious if the unsolicited email contains spelling errors or incorrect grammar.
- The best practice is to not trust supplied links, especially if received in unsolicited emails; use a reputable search engine to look up the address and/or company names and go from there.
- Do not reply with any personal, confidential or financial information to 'verify' your identity.
- Monitor your credit card and bank statements. If you believe you have been a victim of phishing contact your local police to get advice and to file a complaint.
- Do not click on "Unsubscribe" in a spam/ phishing email – this lets the spammers know they have hit a "live" address and you will get more emails of this type.
- If you believe the email communication to be valid, contact the company directly.
- If you are unsure what to do when a suspect email is received, best practice is to delete it.

When should I report a spam/phishing email?

- When it appears to come from a legitimate source.
- When it is threatening.
- If you have clicked on a link and/or provided your password.