PDA

FACT SHEET

Fundamentals to Countering Fraud

Phishing

What is Phishing?

Phishing is a broad term for any fraudulent messages that aim to trick its receivers into revealing sensitive info

The attacker usually 'spoofs' (alters) their address/number to disguise themselves as someone known to the victim, or someone in a position of influence.

Protecting yourself

- Never reveal sensitive information to any unknown persons via email/message, or follow any unknown links.
- Email or call the person directly who has requested payment/sensitive information.
- Make sure a spam filter is enabled on your email account.
- Enable Two Factor Authentication on all possible accounts.

Types of Phishing

Many terms have been coined for phishing targeted at particular victim types or methods of distribution.

Examples of distribution methods

- Smishing – phishing conducted via text messages or messaging services.
- Vishing – phishing conducted via voice, usually by phone.
- Page hijack/clone – phishing conducted via an altered website that looks legitimate, but gathers the victim's data.
- Clone Phishing – phishing conducted via a cloned, previously legitimate email which has had it's attachments/links changed.

Examples of victim types

- Spamming - phishing conducted without any particular target in mind.
- Spear phishing - phishing aimed at a particular person or organisation.
- Whaling – phishing aimed at a CEO, manager or senior official.