Phriendly Phishing

Spear Phishing

A personalised phishing attack targeting a specific individual or organisation.

Understand how spear phishing works to protect yourself, your family & your organisation.

Step 1: The Homework

Scammers start by researching their target. Social media is a common place for scammers to discover specific information about you.

Stay Safe Be careful what sensitive information you post on social media (i.e. birthdays, addresses, etc). Configure your privacy settings to limit visible information.

Step 2: The Scam

Scammers send you a personalised email. To make it seem legit, they'll include your name, personal information and even your interests.

Watch Out Remember to Scan for S.C.A.M. (see below) before clicking on links or opening attachments sent to you.

Step 3: The Click

If you've clicked on a link, you've likely unwittingly installed malware on your device, or handed scammers your personal details.

Be Vigilant Recognise spear phishing tactics including a sense of urgency, authority or appealing to your curiosity before you click.

Step 4: The Breach

If you've been phished, the repercussions could include time and money to fix the damage, loss of reputation or possible fines.

Protect Yourself If you receive a phishing email, report the phish to your IT Department at work, or Scamwatch at home.

Don't forget SCAN for S.C.A.M.

SENDER Check for unusual domain names and organisations using free email services.

CONTENT Red flags might include poor spelling, incorrect grammar or a sense of urgency.

ACTION Hover over links before clicking; check for IP Addresses in URLs; don't fill in forms or open suspect attachments.

MANAGEMENT Don't reply or take any action on the email. Notify your IT Department instead.

Phriendlyphishing.com | support@phriendlyphishing.com

PUBLIC