Five tips to prevent phishing

Five tips to help you identify malicious activity

A typical phishing attack will comprise scammers sending thousands of emails to people. They may ask for personal information, bank details or try and lure people to scam websites. They may even try to trick you into sending money or steal your details to sell on. They may appear genuine, from someone that you know or a senior colleague.

In this guide we share five tips about how to prevent phishing and share some indicators to help you identify a malicious attempt.

1. Be aware of new phishing techniques:

Be aware of how someone might target your organisation and make sure that your team understands. Follow the media for phishing attack reports, as the attackers might come up with new techniques for luring users into a trap. Do you or your staff know where to get help?

2. Don’t give away your personal details:

Scammers use publicly available information shared on your website and social media accounts, so they may look genuine. Always be alert if an electronic message from a seemingly trustworthy source asks for your credentials or other sensitive details. If necessary, verify the contents of the message with the sender or the organisation they seemingly represent, using contact details known to be genuine rather than details provided in the message.

3. Think twice before you click:

Always have a suspicious mind. If a suspicious message provides a link or attachment, don’t click or download. Doing so might lead you to a malicious website or infect your device with malware. If it sounds too good to be true, then it probably is.

4. Check your online accounts and footprint regularly:

Proactive action is key, so even if you don’t suspect that an attack has taken place, or that someone is trying to steal your credentials, check your banking and other online accounts for suspicious activity. Just in case.

5. Use a reliable anti-phishing solution:

Your IT support company will be able to advise you not only about the best solutions, but also how to deploy and manage them. They will also know how to configure your staff accounts so if you are a victim of an attack, then the potential damage is reduced. The use of two-factor authentication (2FA) on email accounts, for example, is vital so that even if your password is known, attackers won’t be able to access that account.

Apply these techniques and enjoy a more secure and productive working environment.

Contact us:
support@itg.uk.com
01625 613 633
www.itg.uk.com