Calder iT Ltd
SUPPORTING BUSINESSES THROUGH THEIR IT JOURNEY

Phishing Factsheet

Welcome to Your Phishing Factsheets

You've got these 3 fact sheets because you care about protecting your business and your staff's personal data from phishing attacks. This document provides key information along with practical steps to help you and your team safeguard your organisation against potential threats.

What is Phishing?

Phishing is a type of cybercrime where attackers deceive individuals into revealing sensitive information, such as passwords, credit card numbers, or other personal details. This is typically done through fraudulent emails, messages, or websites that appear to be from legitimate sources.

phishing via email examples:

Tech Support Scams: **These emails claim there's an issue with your computer and urge you to download a "fix" that is actually malware.**

Tax Refund Scams: **Posing as HMRC or other financial departments, these emails promise a refund but aim to steal your financial details**

Suspicious Activity Notices: **These emails warn of suspicious activity on your account and prompt you to verify your identity by clicking a link**

Social Media Phishing: **Emails that appear to be from social media platforms asking you to verify your account or reset your password.**

Payment Confirmation Scams: **Fake receipts, invoices or charges that prompt you to click on a link to dispute the charge, or make a payment.**

Always be cautious of unsolicited emails, especially those that create a sense of urgency, ask for personal information, or want you to click on a link. If you're unsure about an email, it's best to contact the organisation directly using a known, trusted method, (**do not reply to the email**) or contact Calder IT to check the origin of the email.

Phishing Factsheet

Phishing via text message

Phishing via text often called smishing (a combination of "SMS" and "phishing"), involves cybercriminals sending harmful links or requests for personal information through text messages.

Signs that your text message is smishing:

Unknown Sender: The message comes from a number you don't recognise.

Urgent Language: The message creates a sense of urgency, such as claiming your account will be locked if you don't respond immediately.

Suspicious Links: The message includes a link that looks unusual or doesn't match the supposed sender's website.

Social Media Phishing: Texts that appear to be from social media platforms asking you to verify your account or reset your password.

Requests for Personal Information: The message asks for sensitive information like passwords, credit card numbers, or account details.

If you receive a suspicious text, it's best not to click any links or provide any information. Instead, you can report the message to your mobile provider by forwarding it to 7726 (which spells "SPAM" on an old fashioned phone keypad) in the UK.

Calder iT Ltd
SUPPORTING BUSINESSES THROUGH THEIR IT JOURNEY

Phishing Factsheet

Phishing via WhatsAPP

Phishing via WhatsApp, often referred to as WhatsApp phishing, involves scammers using the platform to deceive users into revealing sensitive information or installing malware.

Signs that your WhatsApp message is phishing:

Account Hijacking: Scammers pose as a friend and ask for your WhatsApp verification code, which they use to hijack your account. Once they have control, they can impersonate you to scam your contacts.

Fake Tech Support: Scammers pretend to be WhatsApp support and ask for personal information or direct you to malicious websites.

Gift Card Scams: Messages claim you've won a gift card and ask you to click a link to claim it. The link often leads to a phishing site designed to steal your information.

Emergency Scams: Scammers impersonate a friend or family member in distress, asking for money or personal information

To protect from these scams:
Verify Contacts: Always verify the identity of the person contacting you, especially if they ask for sensitive information.
Avoid Clicking Links: Be cautious of unsolicited links and attachments.
Enable Two-Step Verification: Add an extra layer of security to your account.
Report Suspicious Messages: Use WhatsApp's reporting feature to flag suspicious messages.