POLICE SCOTLAND
POILEAS ALBA

Cybercrime Harm Prevention Team

Forms of phishing

Police Scotland

July 2024

PHISHING

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a suspect website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to millions of people, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

SMISHING

Smishing simply uses text messages instead of email, the name is a combination of ‘SMS’ and ‘Phishing’.

These are untargeted text messages sent to many people, asking for sensitive information or encouraging them to visit a fraudulent website.

These text messages may purport to be from your bank, asking you for personal or financial information such as your account details.

Typically, attackers want the recipient to open a URL link within the text message, where they then are led to a fraudulent website or app which prompts them to disclose their private information.

There are a few things to keep in mind that will help you protect yourself against ‘smishing’ scams.

- Do not respond. Even prompts to reply like texting “STOP” to unsubscribe can be a trick to identify active phone numbers.
- Don’t be rushed. Approach urgent account updates and limited time offers as caution signs of possible smishing.
- Legitimate institutions don’t request account updates or login info via text. Call your bank using the number on the back of your bank card to confirm messages from them are genuine.
- Avoid using any links or contact information in the message.

VISHING

Vishing is executed over telephone calls. Criminals impersonate a person or business and try to convince you to provide your personal details like credit card numbers, bank account details and passwords over the phone. The name 'vishing' is a combination of 'voice' and 'phishing'.

These scams may start online where the criminal will obtain a phone number through a phishing email. Before calling criminals can create fake caller ID profiles so that the phone numbers they're calling from seem legitimate and from a local area code or a trusted business.

Here are two of the most common scams to look out for:

Technical Support Scams:

Criminals may pose as technical support personnel from large companies like Amazon or Microsoft. The cybercriminal would call you claiming to have detected a harmful virus on your phone or computer or to alert you of an important software update. They will go on to try and convince you to share personal information or give them remote access to your device.

Purporting to be your Bank:

A common vishing scam is when attackers pose as representatives from banks or financial institutions. The cybercriminal may tell you there's an issue with your account or a recent payment you made. They will go on to trying to convince you into sharing account details or transfer funds to another account.

Here are a few simple measures you can take to prevent against falling for one of these scams:

- Avoid answering phone calls from unknown numbers. Instead, let them go to voicemail.
- Don't share your personal information over the phone. Banks, credit card companies and service providers will never call asking for sensitive information.
- Hang up immediately if a caller from a purported reputable company sounds suspicious. Then call the company yourself, so you can be sure it's legitimate or not.

QUISHING

Quishing is a form of phishing which uses QR codes to lure you to fraudulent websites. This is done by creating a malicious QR code which mimics a legitimate one. Users are then redirected to a malicious website or prompted to download a rogue application, believing it to be from a trusted source. Then they are prompted to provide personal information such as banking details.

The following tips will help to avoid falling prey to this scam:

Scrutinize the QR code itself. Watch for unusual designs, pixilation or errors in the code structure. This can include letters or symbols written in tiny font between the square barcodes.

Verify the source. Confirm via a separate medium e.g., text message, voice call, etc., that the message is legitimate.

Assess the degree of urgency and emotional tone. A sudden or unprompted request for personal information may be a sign of a 'quishing' attack. These scams also tap into emotion to elicit a fast response, so consider whether the message expresses a sense of fear or curiosity.

Always check the URL before scanning. If it appears random or doesn't match the supposed sender, it could be fraudulent. Typically, users can see a preview of the link before clicking as their cameras scan over the code.

Be cautious of QR codes asking for sensitive info or prompting auto-downloads. Genuine codes generally direct to a website for information rather than requesting personal data up front.

Never scan a QR code from an unfamiliar or unexpected email.

Be wary if a QR code takes you to a site that asks for personal information, login credentials or payment.

HELP AND SUPPORT

Police Scotland – Report any fraud or other crime to the police by visiting the Police Scotland website or phoning 101 – Contact Police Scotland - Police Scotland

Crimestoppers UK – is a charity which gives you the power to speak up to stop crime. By phone and online, 24/7, 365 days a year – Crimestoppers in Scotland | Crimestoppers (crimestoppers-uk.org)

Victim Support Scotland – Support victims of crime, witnesses and their family members, regardless of who they are and their circumstances. Their service is independent, free, non-judgemental and confidential. They offer bespoke support, personalised to the needs of each individual – Home - Victim Support Scotland

REPORTING

If you have received an email which you're not quite sure about, forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk

Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.