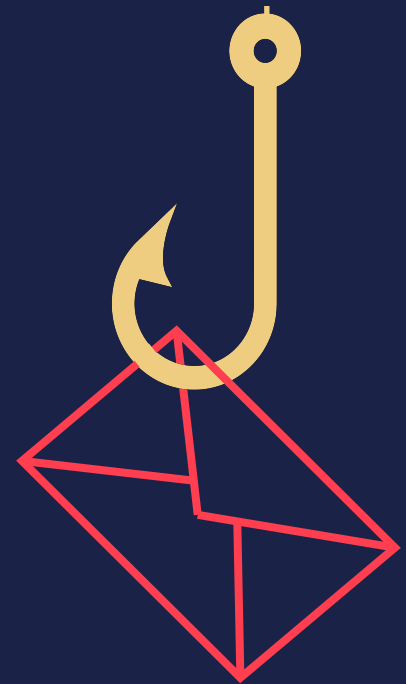


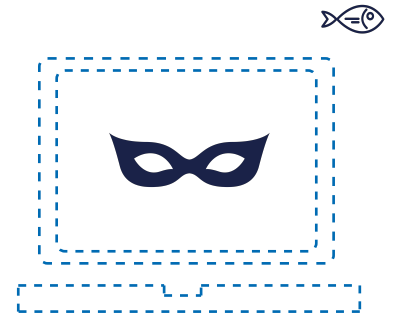
SOMETHING PHISHY...

A guide to recognising and
avoiding phishing attacks



WHAT ARE PHISHING ATTACKS?

Phishing attacks are designed to trick you into revealing sensitive information or installing malware (including ransomware) on your devices. They are carefully crafted to look genuine and appear, on the surface, to be from a legitimate source.



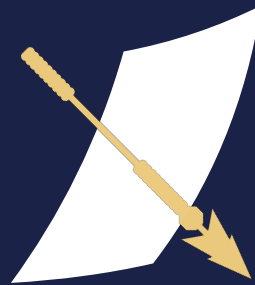
PHISHING METHODS

MASS PHISHING



The most common type of attack, using little personalisation. These emails usually appear to come from a recognised service provider, like a bank or HMRC and are cast out to a huge amount of email addresses.

SPEAR PHISHING



A targeted attack which uses found or stolen information to tailor an email for an individual or group in order to make it more convincing.

WHALING



A personalised attack aimed at figures of authority in a company, with the goal of stealing their login information. This can then be used to impersonate the individual and authorise or direct fraudulent payments.

PHISHING EMAILS

Phishing emails can often look convincing initially, but there are some tell-tale signs to look out for.



The sender address spoofs a known brand.

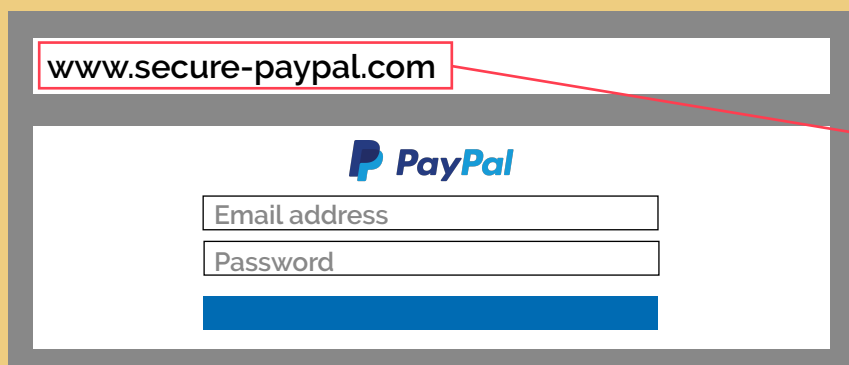
Generic greeting.

Unprofessional tone and grammatical errors.

Link text and the web address do not match. These links may lead to sites containing malware or fake sites that will steal your login or financial information.

Request for sensitive information.

Scare tactics, designed to panic you into action.



Links in emails often lead to impostor websites that look real. These may have addresses that spoof those of a trusted organisation.

TARGETED PHISHING EMAILS

Targeted phishing emails can also appear to come from colleagues, suppliers and other close business contacts.


Targeted phishing emails may appear to come from legitimate sources.

Compressed attachments. Common file attachments like .doc, .xls and .ppt can contain malicious macros.

Whaling and spear phishing emails can often contain personalised information, such as the names of friends or co-workers.

Request to open an attachment or click a link.

From: Anne Smith <asmith@anothercompany.com>
To: John@yourcompany.com
Subject: BACS Remittance No 883457210

 883457210_Your_Company.zip

Dear John,

I was passed your details by your Finance Director Andrew Mitchell.

We have arranged a BACS transfer to the Your Company bank account in the amount : (£) 3187.00.

Please see full information on the attached document.

Kind Regards,
Anne Smith
Office 02076 547900
Another Company



Common phishing emails:

Here are some of the most common phishing emails we see:

- OneDrive file share links - this also extends to Google Docs and Dropbox
- Password update requests
- Unusual activity on your account
- Multi-factor authentication set up (typically 'from' Microsoft)
- Requests for payment / fake invoices
- Messages from HR teams
- Account upgrades
- Free advice



VISHING

Voice phishing is referred to as Vishing. Criminals make telephone calls to gain access to private and financial information.



The caller will already have genuine information like your name, address, phone number and bank details.



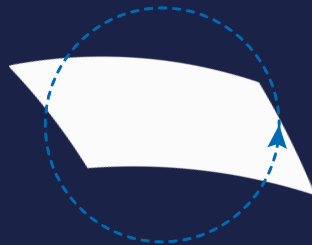
Criminals will create a sense of fear and urgency - often that your money is in danger and you need to act quickly.



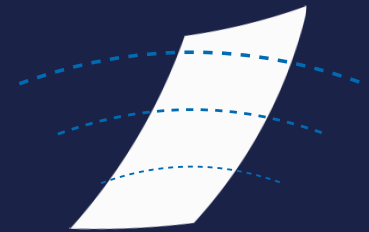
Fraudsters sometimes offer unsolicited prizes or present offers that are too good to be true.



The phone number may be spoofed so it looks like the call is coming from legitimate source.



Criminals can sometimes hold your telephone line, so if you hang up and call again on the same line, you might get put straight back through to them.



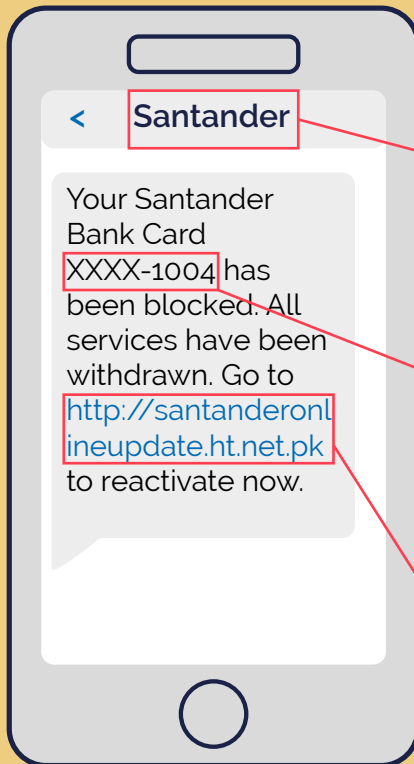
There may be fake background noise to make it appear as if the call is coming from a call centre.

If you receive a suspicious phone call, **hang up**. Search for the apparent callers details on their website or on official documentation, and call them back on a different device to confirm if the call was real.

If you get an unexpected call from your bank, you can hang up and dial 159. You will safely be connected to your bank, and 159 cannot be spoofed.

SMISHING

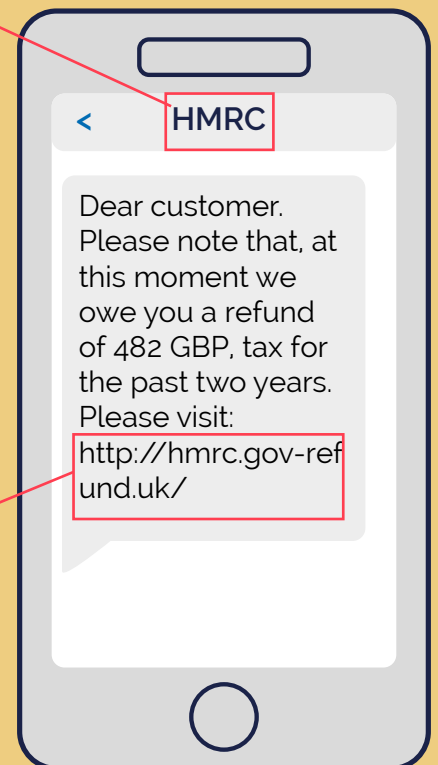
SMS phishing is similar to email phishing, but uses text messages. As with vishing and spear phishing it can be personalised.



Numbers can be faked to make it seem like they are from legitimate organisations.

Criminals sometimes use digits from your card to pressure a response.

Messages can use fear or financial gain to push you towards fake websites that may either attempt to harvest personal data or infect your phone with malware.



If you receive a scam SMS, you can report it by forwarding the message to **7726** for free.



QUISHING

Quishing is phishing using QR codes. QR code scams are popular because you use your mobile phone which typically has less protection than your laptop.

Offline:

There are two things to consider with QR codes in the physical world:

- 1) Is the QR code attached to a legitimate source?
- 2) Has the QR code been replaced?

Examples:

- 1) A fake event flyer created to generate sign up with financial information through a QR code.
- 2) A malicious QR code sticker has been placed over the one you would scan to pay for your car parking.



Online:

Online, QR codes are often used to encourage app downloads, verify accounts and more.

Criminals will replicate emails, or put out malicious QR codes in the hope that you will scan them and follow any instructions required.

Don't scan any QR code if you can't confirm the source.

Instead, search for the information in your browser or contact the sender to confirm.

From: Microsoft <microsoftsupport@microsoft.com>
To: Rob@yourcompany.com
Subject: Multi-Factor Authentication Setup

 Microsoft

Microsoft Multi-Factor Authentication 2FA Set Up.

Your 2FA multi-factor settings require review. Follow the steps below to verify. Scan the QR code with your smartphone camera to re-authenticate your password security.




1. Scan the QR code using your phone camera.
2. Login to your account, then go to settings.
3. Review and verify information and save changes.



SOCIAL MEDIA PHISHING


Criminals use social media to launch attacks that aim to steal personal data, spread malware or even hijack accounts.

What to look out for on social media:




 **Steve Jones** 2 hr


Had a few issues so I set up a new account.


 **Rosie @rosiet3** 1 hr

My @Barclays account has locked me out!



  


Admin 

Hi John, we have spotted a security threat on your account with multiple log in attempts. We recommend updating your password: <http://facebook.securitypasswordupdate/12864/>




 **Steve Jones** 30 mins

Check this out, it looks great: <http://bit.ly/2wXBk4d>

 **Barclays Support @ask_barclays** 2 mins

@rosiet3, Hi Rosie, we apologise for this. To regain access visit: <http://bit.ly/2gpBkz2>

Criminals set up replica accounts to contact the victim's followers to tell them that their legitimate account has been abandoned. They will then send messages from the new account to try and trick the victim's followers into clicking on links to websites which may steal data or contain malware.

In 'angler phishing' attacks, scammers steal branding and create fake customer service accounts. These are then used to respond to genuine user support requests, directing them to legitimate looking but fraudulent malicious websites.

Scammers will also attempt to imitate website admins with the aim of tricking people into giving up passwords and other sensitive information.



On LinkedIn, criminals will set up fake profiles to send connection requests and attempt to message you, which ultimately will turn out to be a scam.

Before you accept a connection request, check the full profile. Pay attention to their work and education history, as well as incomplete information. The best solution: **don't accept the request if you don't know them.**

HOW TO STAY SAFE

Zero Trust

Adopting a zero trust strategy literally means trust nothing. You should validate the source of every email, SMS, telephone call etc., before you take action.

Don't click on links or download attachments

Don't engage with anything in the communication until you have confirmed it is safe to do so.

Contact the sender directly

Use details on the apparent sender's official website and documentation to try and confirm legitimacy of the contact. If you are contacted on a phone, try to use a separate device to get in touch in case the line is being held.

Be suspicious

Look carefully at any unsolicited communication, particularly if it encourages you to take urgent action or it seems out of character for the sender.

Report any suspected phishing activity

At work, take the below steps if you receive or action a phishing email:

You received a phishing email

- 1) Do not action the phish. Take a screenshot of the email and send this to **all** of your colleagues.
- 2) Contact us to report the suspected phishing activity.

We can then take action, including removing the email from all user mailboxes.

You clicked a phishing email

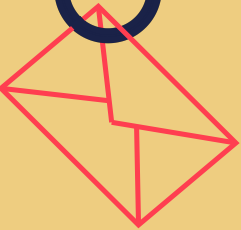
- 1) Contact us immediately to let us know. We can then take action and check for any further incidents.
- 2) Let the appropriate person within your organisation know. This could be a senior manager or internal IT support.

Contact us on 01603 709300.

On your personal device, please contact Action Fraud at: www.actionfraud.police.uk

Stay up-to-date

We often share the latest scams and tips to avoid them on our website and social media channels.



To learn more, contact us today
on 01603 709300

www.breakwaterit.co.uk