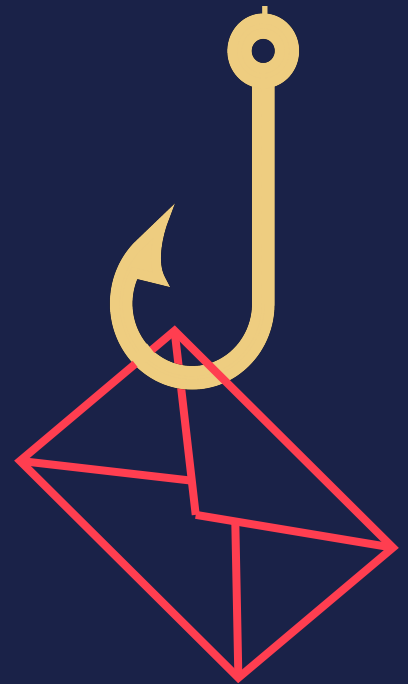


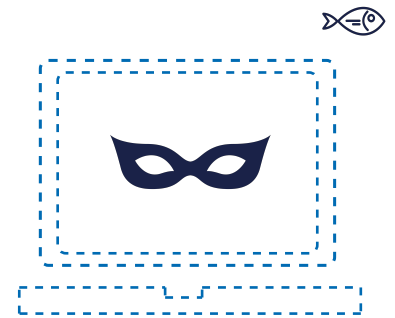
SOMETHING PHISHY...

A guide to recognising and
avoiding phishing attacks



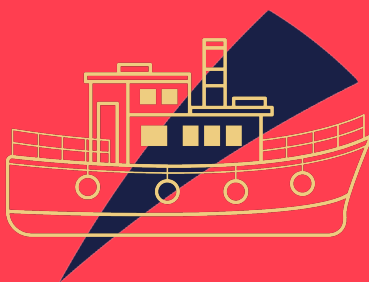
What are Phishing Attacks?

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.



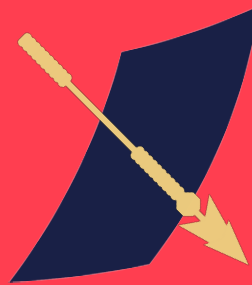
Phishing Methods

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.

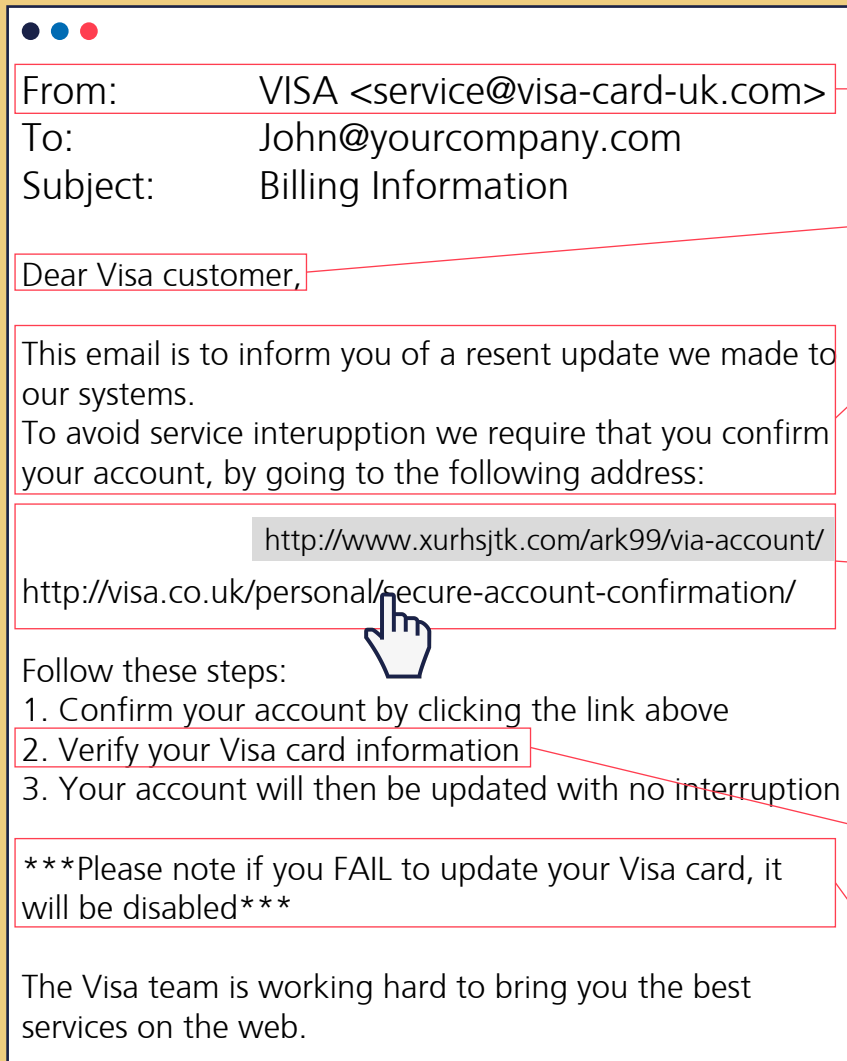
WHALING



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.



From: VISA <service@visa-card-uk.com>
To: John@yourcompany.com
Subject: Billing Information

Dear Visa customer,

This email is to inform you of a resent update we made to our systems.
To avoid service interruption we require that you confirm your account, by going to the following address:

<http://www.xurhsjtk.com/ark99/via-account/>
<http://visa.co.uk/personal/secure-account-confirmation/>

Follow these steps:

1. Confirm your account by clicking the link above
2. Verify your Visa card information
3. Your account will then be updated with no interruption

Please note if you FAIL to update your Visa card, it will be disabled

The Visa team is working hard to bring you the best services on the web.

The sender address spoofs a known brand.

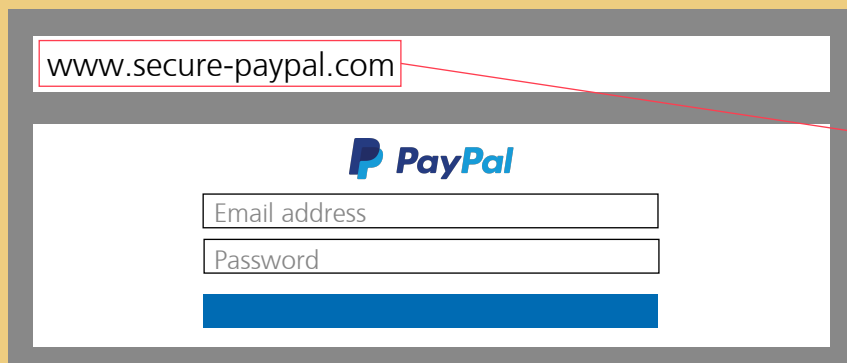
Generic greeting.

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.



www.secure-paypal.com

 PayPal

Email address

Password

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.

Whaling and spear fishing 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 enclosed.

Kind Regards,
Anne Smith
Office 02076 547900
Another Company

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



Security Warning

Macros have been disabled

Enable Content



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.



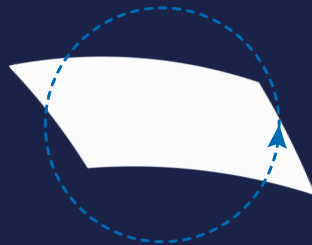
Criminals will create a sense of fear and urgency - often that your money is in danger and you need to act quickly.



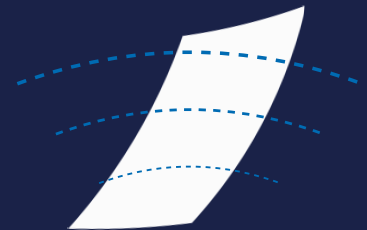
Fraudsters sometimes offer unsolicited prizes or present offers that are too good to be true.



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



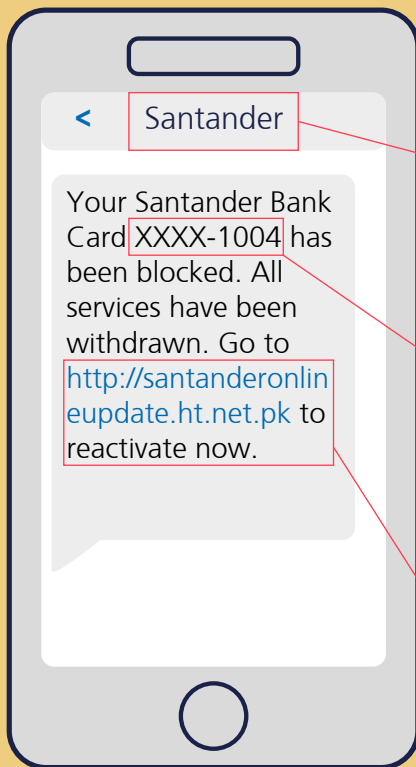
Criminals can sometimes hold your telephone line, so if you hang up and call again on the same line, you might get put straight back through to them.



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

Smishing

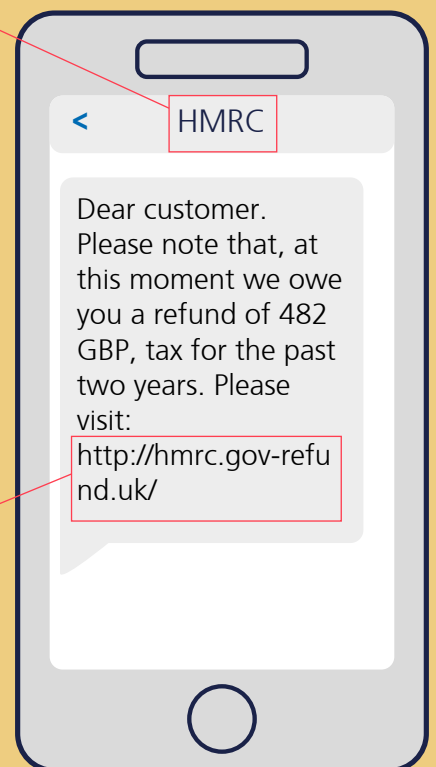
SMS phishing is similar to email phishing, but uses text messages. As with vishing and spear phishing it can be personally targeted.



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.





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.




 Steve Jones
30 mins


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




 Rosie @rosiet3
1 hr


My @Barclays account has locked me out!

 Barclays Support
@ask_barclays 2 mins

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

Admin 

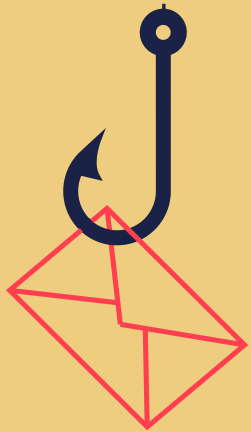
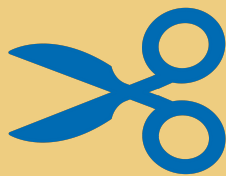
Hi John, we have spotted a security threat on your account with multiple log in attempts. We recommend updating your password:
<http://facebook.securitypasswordupdate/12864/>

Criminals set up replica accounts and then contact the victim's friends and followers to tell them that their previous account has been abandoned. They will then use messages sent from this 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.





How to Stay Safe from Phishing

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.

Don't click on links or download attachments

If you suspect something is wrong, don't engage with anything in the communication.

Contact the sender directly

Use details on the apparent sender's official website and documentation rather than any given in the communication to try and ascertain the legitimacy of the message. If you are contacted on a phone, try to use a separate device to get in touch in case the line is being held.

Report any suspected phishing activity

At work, contact us here at Breakwater IT: 01603 709300 for any suspected phishing activity on your systems and we can take action on your behalf. On your home device, please contact Action Fraud at www.actionfraud.police.uk

To learn more, contact us today
on 01603 709300

www.breakwaterit.co.uk