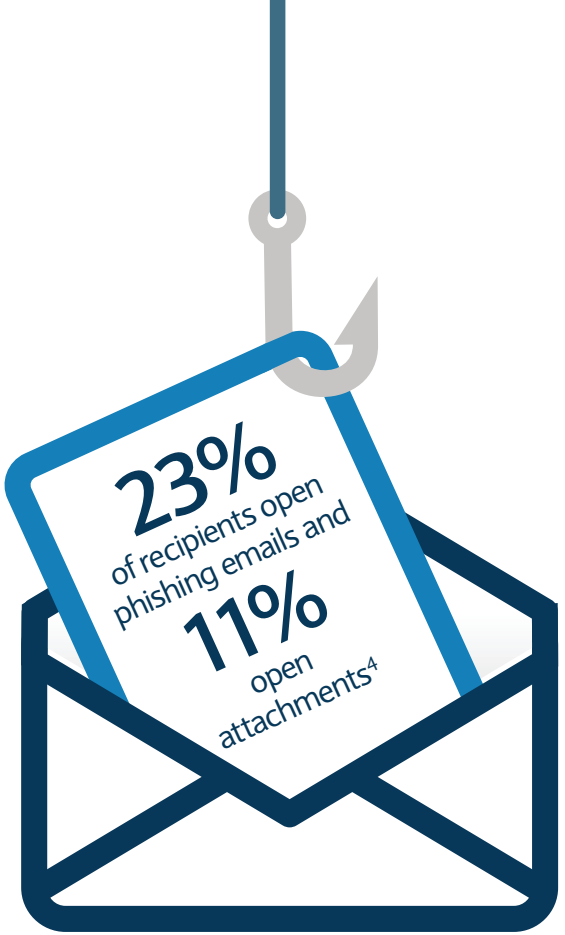


Phishing

Phishing involves a fraudster, posing as a legitimate source, sending emails or letters that aim to trick people into divulging sensitive information or transferring money into other accounts. The emails typically contain a link to a fake website, which will request that you enter financial information. Alternatively, emails may contain an attachment in the form of a document, form or notification.

Equally, the email may be designed to contain and deliver malware via an attachment or a link. If the link is clicked or the attachment opened, the criminal will be able to gain access to your system.

Vishing

Vishing (vocal phishing) involves a fraudster phoning a company in order to convince a member of staff to reveal sensitive company information or make a payment.

Most commonly, fraudsters make an unsolicited call pretending to be from your bank, so they can ask you to reveal confidential information or make payments to account details provided. Cases of fraudsters impersonating the CEO of the victim's company have also been on the rise, while other tactics include impersonating the police, utility providers, delivery companies or other service providers. They may claim that your account or card has been compromised, or that a payment has been made by the business using incorrect bank details.

Caller IDs or numbers on display are relatively easy to change or spoof. Fraudsters have been known to convince people a call is genuine by getting them to cross-check the incoming call number with the official number of the bank.

Smishing

Smishing is where a fraudster targets a victim via a text purporting to be from their bank, in order to convince them to reveal sensitive financial information or transfer money into other accounts. The text often contains a phone number, which connects you to the fraudster. As with vishing, details can be spoofed, so it can seem as if the texts are coming from a legitimate source and they can even be inserted into genuine text communications with the bank.

[4]Data Breach Investigations Report. [5]McAfee, 2016.

Protecting your business against phishing, vishing and smishing

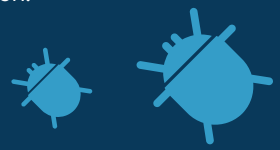
- Do not assume a caller is genuine because they know information about you or your company – fraudsters are skilled in collecting enough information to sound convincing and can change caller display IDs to a genuine looking number
- Never enter any personal or security information on a site accessed through a link in an email
- Never click on links or open attachments from senders you are unsure of
- If you are suspicious, terminate the call and call back using your usual contact number, and not one provided by the caller
- On sites that require you to input sensitive information, look for 'https' in the website address – the 's' stands for 'secure'
- Remember that your bank may ask you for some information, but will never ask for your full password or PIN, provide you with details to make a payment, or request that you grant them access to your systems or PC.

Case study

The accounts department at XYZ Ltd received an email instruction purporting to be from the director for a payment. The director often made payment requests this way.

When replying to the director's email, the return address matched the director's email exactly, providing the accounts team with assurance of its authenticity.

Two payments totalling £125,000 were made. The fraud was identified when the accounts team later called the director, who advised he knew nothing of the instruction.



"Intelligence suggests that criminals have recently increased their focus on phishing emails purporting to be from major online retailers and internet companies, brands which a large proportion of recipients are likely to use. These emails are increasingly sophisticated and attempt to trick recipients into giving away personal or financial details, or into downloading malware."

Financial Fraud Action (FFA) UK
Year end 2016 Fraud Update