Phishing, Vishing and Smishing - What are these?

Any website, online service, phone call or text message that poses as a company or brand you recognise.

Any contact like this is designed to convince you to hand over valuable personal details or your money, or download something that infects your computer.

The three terms are all plays on the word 'fishing', in that the fraudsters fish for potential victims by sending emails, social media messages or text messages or making phone calls with urgent messages in the hope of persuading someone to visit the bogus website.

Protect yourself

- Don't assume anyone who's sent you an email or text message – or has called your phone or left you a voicemail message – is who they say they are.
- If a phone call or voicemail, email or text message asks you to make a payment, log in to an online account or offers you a deal, be cautious. Real banks never email you for passwords or any other sensitive information by clicking on a link and visiting a website. If you get a call from someone who claims to be from your bank, don't give away any personal details.
- Make sure your spam filter is on your emails. If you find a suspicious email, mark it as spam and delete it to keep out similar emails in future.
- If in doubt, check it's genuine by asking the company itself. Never call numbers or follow links provided in suspicious emails; find the official website or customer support number using a separate browser and search engine.

Spot the signs

- Their spelling, grammar, graphic design or image quality is poor quality. They may use odd 'spe11lings' or 'cApiTals' in the email subject to fool your spam filter.
- If they know your email address but not your name, it'll begin with something like 'To our valued customer', or 'Dear...' followed by your email address.
- The website or email address doesn't look right; authentic website addresses are usually short and don't use irrelevant words or phrases. Businesses and organisations don't use web-based addresses such as Gmail or Yahoo.
- Money has been taken from your account or there are withdrawals or purchases on your bank statement that you don't recall making.

How it happens

Phishing, vishing and smishing are done in many different ways. In the end the aim is always to trick you into thinking that you're giving up personal information or making payments with someone you can trust such as your bank, a government agency or a business or brand name.

The fraudsters will use your details to steal your identity or simply take the money you've paid and break all contact.

Source – ActionFraud Police UK

Websites

You may find a website pretending to be a well-known company, organisation or service. The aim of these websites is to convince you that you're using a real online service so that you hand over your personal or banking details or send money.

Emails

Phishing emails encourage you to visit the bogus websites. They usually come with an important-sounding excuse for you to act on the email such as telling you that your bank details have been compromised or claim they're from a business or agency and you're entitled to a refund, rebate, reward or discount.

The email tells you to follow a link to enter crucial information such as login details, personal information, bank account details or anything else that can be used to defraud you.

Alternatively, the phishing email may try to encourage you to download an attachment. The email claims it's something useful, such as a coupon to be used for a discount, a form to fill in to claim a tax rebate or a piece of software to add security to your phone or computer. In reality, it's a virus that infects your phone or computer with malware, which is designed to steal any personal or banking details you've saved or hold your device to ransom to get you to pay a fee.

Social media

Facebook, Twitter and other social media channels are also used to direct you to a spoof website. Fraudsters create accounts that have similar usernames and profile pictures to official accounts to trick you into thinking you're dealing with someone you can trust.

Official accounts are 'verified' – they come with a checkmark icon next to their name, meaning they've proved themselves as the official company to the social media channel.

Phone

Some fraudsters will call your landline or mobile, pretending to be from your bank, building society, a government agency or someone you do business with. This is known as **vishing** (voice + fishing).

Alternatively, they'll send you a text message that asks you to reply with your personal or banking details, or to call or text a premium-rate number they have created to run up a large bill. This is called **smishing** (SMS + fishing).

How to report it

Report it online or call 0300 123 2040

Source – ActionFraud Police UK