How to deal with fraudulent emails

Phishing is a common kind of online fraud, but you can avoid getting caught by following some simple advice. Improved security in modern operating systems and web browsers mean that online malware is a much-reduced threat these days.

But these improvements have a flip side: web villains now find it far simpler to simply trick personal information out of you in order to steal money. The practice is known as 'phishing', since it's essentially a case of baiting a digital hook and waiting for someone to bite.

Here's what you can do to avoid getting caught out.

Step 1: What is a phishing email?

Phishing emails differ from ordinary spam because they ask for personal information such as login details for an online service or credit card details. They do this by pretending to be messages from the service itself, often by claiming there's a problem with your account and that you need to confirm your details by clicking a link.

The most sophisticated phishing emails can be very convincing, but there are almost always telltale signs that give the game away.

Step 2: Spotting a phishing email

It's important to remember that no reputable organisation should ask for personal details via email, so that should always be a giveaway for a phishing email — assuming it gets through your email application's spam filter in the first place, of course.

BT, for example, never sends emails to customers asking to verify account details, and they would never send an email that includes an attachment.

Spelling mistakes and poor grammar are also signs of a scam, as is the sender's email address. Your email application may show a convincing name for the email sender, but the sender's actual address will almost always give the game away. It may have the words 'undisclosed recipients' or an unknown address in the To and From fields.

Does the email use your name? It's rather unlikely your bank would start an email with "Dear customer". Is the email trying to create a sense of urgency or panic? A common tactic.

Has it come from an organisation you're doing business with now, or have done in the past? If so, just visit their site via your usual method. Never use links provided in the email.

Did the email come out of the blue? If you're not expecting a parcel, or haven't placed an order, be suspicious. Don't be tempted to reply

Is the email grammatically correct and is the formatting of images correct? Large organisations don't normally send emails with poor grammar, spelling or content.

Don't reply to any email you assume to be phishing - and if you are unsure whether an email is genuine or not, simply delete it.

Step 3: Make sure your browser is up to date

If you are completely fooled by a phishing email and click its link, your web browser will almost certainly detect the fraudulent site and block it.

That's why it's essential to always use the most up-to-date version of a web browser — older versions may have weaker anti-phishing protection and may not spot a fake.

Step 4: Check the page

If you end up at a phishing site's 'log in' page without any warning from your web browser, all is not yet lost. You should always check the web address of any site that asks for login information, whether the site is genuine or not.

Fake sites will almost always lack the https:// that shows a web site's login page is encrypted for extra security, but the address itself should also show that the site isn't the real thing — no matter how plausible the page itself might be.

Step 5: Password protect

If you do inadvertently provide login information to a phishing site, it's important to change your password for that service as soon as you realise your mistake — and for any other services that use the same password.

If the site is for a bank or any other service that has access to your financial details, notify them immediately and report the fake site to Action Fraud, the UK's national reporting centre for fraud and internet crime. You can also report phishing attempts that weren't successful.

Step 6: Spam filters

Phishing emails are best marked as 'spam' in your email application and, all being well, you won't see them, or emails like them again.

Many email services offer spam protection, which automatically send many such emails directly to your spam folder.

Step 7: Blocking

Blocking an email address means you won't receive email from the sender again. Many email services provide a facility to block specific senders.