SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

Online Fraud

Although fraud is categorised differently to cyber crime by law enforcement, some of the advice crosses over and can help prevent both. When it comes to fraud, always take time to stop and think it through before you give away any personal information or make a purchase.

Phishing emails and text messages (SMS)

We've had reports of criminals posing as various officials and sending emails requesting that you click on links, which downloads malicious software, to steal your personal information.

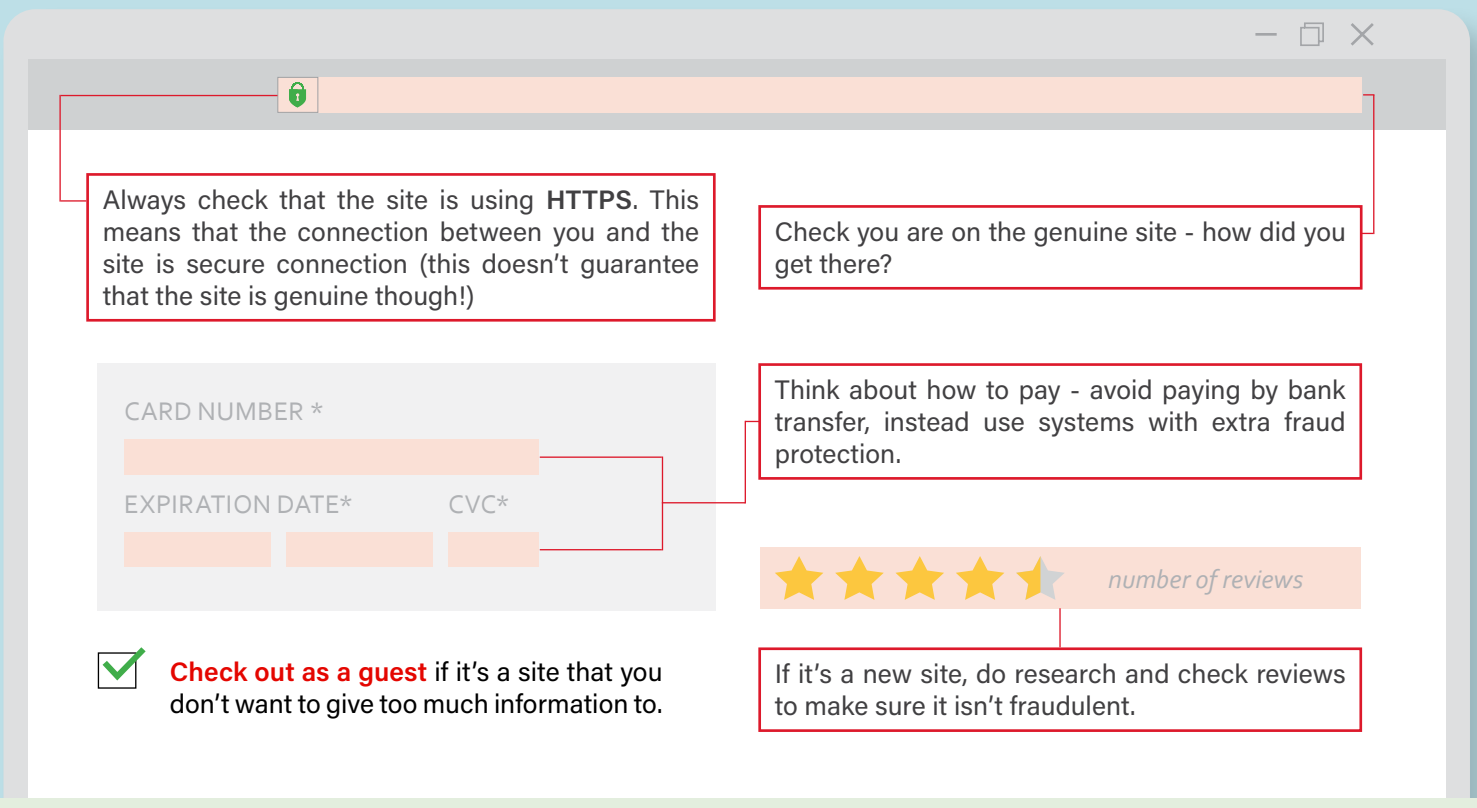
This tactic of trying to persuade a person to download something, or give away personal information is known as **phishing**.

To avoid falling victim to phishing attacks, we recommend that you:

- **Avoid clicking on links** - there is almost always another way
- **Verify the communication is genuine** - e.g. phoning a trusted number
- **Check that the email makes sense** - look at spelling, grammar, mannerisms, context
- **Think about your 'digital footprint'** - what's available about you online e.g. from social media, basicGoogle searches etc.

For further information on phishing, please refer to our **Phishing Advice Sheet**.

Online Shopping



Protecting your devices

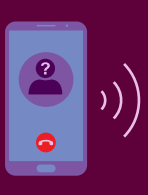
Protecting your devices will help protect you if you do accidently click on malicious links or attachments. It's important that all computers have:

- Updated software and operating systems. Ensure that you apply updates to devices (inlcuding phones) as soon as reasonable possible.
- An active, up-to-date antivirus. This will detect viruses and stop them before any damage is done.
- An active firewall. Most computers have a firewall built in, never disable the firewall, even if a program requests you to do so.

Other types of fraud

Vishing

The telephone equivalent of phishing, vishing is an unsolicited voice call asking for personal or financial information. If you suspect a vishing call, hang up, wait 5 minutes and call the person/organisation on a number you know is genuine.



A text message pretending to be from someone you recognise, for example your bank. These can appear in the same thread as a previous conversation. Never engage with a number, email address or link in a text message. Instead use a number that you know is genuine for example, on the back of your bank card.

Smishing

COVID-19 Fraud

Watch out for phishing emails related to COVID-19 and always go the official government webpage for up-to-date guidance. Criminals are also setting up fake websites to sell products such as face masks and hand sanitiser, so follow the tips above before making any purchases.

A phone call from someone impersonating a computer software company (e.g. Microsoft) or your IT helpdesk. They will report an issue with your computer and ask you to download software to fix it, along with a payment.

Computer Software Service Fraud

For further advice on how to avoid different types of fraud, don't forget to check out the NHS Digital Security Centre.

Reporting

If you are a victim of any type of fraud, please report it to Action Fraud (https://www.actionfraud.police.uk), or to the relevant lead in your organisation. If you make a payment and then suspect it is a scam, please also contact your bank as soon as possible.

If you've spotted a potential phishing email, you can now report it to the NCSC's Suspicious Email Reporting Service (SERS) by forwarding the email to 'report@phishing.gov.uk' - more information can be found on the NCSC's website at https://www.ncsc.gov.uk/information/report-suspicious-emails