Cyber Scams

A look at cyber scams and how to spot them

Cyber Scams

A scam is when someone attempts to take money, personal information or other goods from someone via their phone, laptop or tablet.

We call these criminal scammers.

There are different types of cyber scams. Some of the most typical types are:

Phishing

Fake anti-virus software (Trojan horses)

Formjacking

Spyware

Phishing

Phishers pretend to be someone you might know - a friend, neighbour, someone from school, or your bank.

They try to get you to hand over information or click a malicious link via email, social media or other messaging apps like WhatsApp.

They generally have something urgent they want you to do - money in an emergency, claim a refund, or prevent a bank transaction.

It's important not to click on these links! They will get access to your personal stuff like bank details or information on your identity.

How to Spot Phishing

The most important step in stopping a phishing attempt is to **take your time** reading the entire email or message.

This will help you spot things like **names not being spelled properly, poor grammar** in the text and links that don't lead to the place they should.

Fake anti-virus software

If you're browsing the web and all of a sudden you get a pop up saying that your computer is now infected, chances are it's an online scam.

These fake antivirus software ads and pop ups want you to download their free software, which will only give you a virus malware or ransomware, among other cyber threats.

Only trust virus information from antivirus installed software on your device- and if you don't have any, it's a good idea to install one.

Watch out for any pop ups with flashy lights or that warn you to take action immediately by downloading an application.

Sometimes a pop up will tell you your device has a virus, and you should click on the link to run a virus check. Do not respond, as the link is most likely to install a virus on your device.

Formjacking

This is when scammers create websites which look almost identical to the original:

- **your bank**
- **HMRC**
- **online shopping sites**

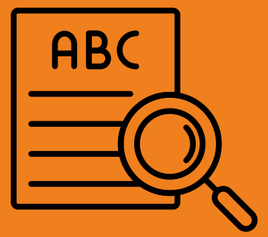
You enter your personal, bank or credit card details. **The information is then stolen and used to access your bank or credit card account.**

Money is then taken from your accounts, often too late for you to stop it happening.

How to Spot Formjacking

Fake sites which are set up for Formjacking have very similar, but not the same web addresses.

The URLs are very similar, however, if you look closely you will notice a small difference, even by one letter or number.



These fake sites often have bad spelling or grammar

They often offer you very special deals with goods, which are much cheaper than usual.

Spyware

Spyware can be downloaded to your device through an internet link or by opening an email attachment.

The software could downloaded without your knowledge or permission.

Spyware can access your mobile phone contacts and photographs. It can switch on your mobile phone camera and take photos, listen in to your telephone calls, and record keystrokes on your devices.

How to Spot Spyware

Your device is using more data than usual.

Your phone makes odd sounds during phonecalls.

Sudden drop in battery life.

Your device is much slower than usual.

Your device reboots itself for no reason.

You are receiving odd text messages, possibly with code language.

Your device shuts down suddenly.

Your device is difficult to shut down.


YOUNG
SCOT
DIGI
KNOW
?