POLICE SCOTLAND
POILEAS ALBA

FRAUD... THE BASICS

A simple guide to help you stay safe online

It often feels like we are bombarded with information every day about the latest frauds and scams.

For example, do you know the difference between phishing, smishing and vishing? If not, don't worry, you're not alone and this guide is for you.

This easy to understand guide gives simple advice on how to stay safe online, explains some of the terms used to describe frauds and looks at some of the techniques used by criminals to make us panic and part with our money.

FRAUD... THE BASICS

STAY SCEPTICAL - STOP AND THINK - COULD THIS BE A SCAM

FRAUD... THE BASICS

Avoid becoming a victim of fraud by making a few easy changes to your online behaviour.

For passwords use three unrelated words, eg fishbooktable; and think of three different words for each account, so if one is compromised the others are safe.

Never give personal or sensitive details out online or over email.

Make sure all devices have up-to-date anti-virus software and a firewall installed.

Keep software and apps regularly updated.

Only download from legal, trusted websites.

Only open emails and attachments from known and trusted sources.

Only ever use websites that start with https://

Avoid using public WiFi hotspots that are not secure; use your 4G data instead. If you have no choice but to use Public WiFi then only use it with a Virtual Private Network enabled on your device.

Regularly back up your data.

Control your social media accounts – regularly check your privacy settings and how your data is being used and shared.

Be cautious of internet chats and online dating – there's no guarantee you're speaking to who you think be extremely cautious if you're asked for money.

STAY SCEPTICAL - STOP AND THINK - COULD THIS BE A SCAM

PHONE FRAUD... THE BASICS

Phone Fraud...The Basics

If you use an online banking app, only use the official app provided by your bank. If in doubt, contact your bank to check.

Only download apps from official app stores, such as Apple iTunes, Android Marketplace and Google Play Store.

Keep your phone's operating system updated with the latest security patches and upgrades. Your operating system provider normally send these.

Never give your mobile banking security details, including your passcode, to anyone else and don't store them on your phone.

Just like on your computer, you can get antivirus tools for your mobile; use a reputable brand.

Be wary of clicking on links in a text message or email. Don't respond to unsolicited messages or voicemails on your phone. Your bank will never email or text to ask for your PIN or full password.

Some Examples

Text scams offering you money for an accident you may have had is often a ploy to get your personal details. Don't reply, even by sending a 'STOP' text.
Simply delete the message.

You may get a text or advert encouraging you to enter a competition for a great prize. The scammers will charge extremely high rates for the messages you send them, as high as £2 per text message. **Don't reply.**

'Trivia scams' involve you answering general knowledge questions to win a prize. If you try to claim your prize, you may have to call a premium-rate number and listen to a long recorded message, designed to keep you on the line. **Don't phone back to claim.**

'SMiShing' (SMS phishing) is when a scammer texts asking for personal or financial information. The message may appear to be from a legitimate company, like a mobile phone provider, but legitimate companies never ask you to provide sensitive information by text. Don't reply to these texts. **Simply delete them.**

INTERNET FRAUD... THE BASICS

Internet Fraud...The Basics

Scammers put programs on your computer that can steal, wipe or lock your data. To prevent this, have antivirus software and a firewall installed and keep it up to date.

Scammers defraud people using spam emails. Simply delete the email without opening or replying to it.

Any email you get from someone you don't know is likely to be spam.

Online marketplaces are used by scammers. Scammers will try to steer you away from online sites and get you to use unusual payment methods.

Adverts and websites can be very sophisticated so do some research to make sure everything makes sense.

Be careful of official-looking but bogus websites that claim to help you apply for passports, visas and driving licences.

Some Examples

There are lots of ways scammers gain personal or financial information from their victims, such as:

Phishing, where an email that seems to be from a legitimate company asks you to give your personal details

Vishing, where either an automated phone message or a cold-caller who seems to be from a legitimate company asks you for personal details

Spear Phishing, which focuses on an individual or department in an organisation; the email appears to come from a legitimate organisation

Using these methods, scammers ask for information such as login details and passwords, or install malware on your computer.

The most common scams at the moment are for:

- concert and event tickets
- residential and holiday lettings
- dating and romance
- vehicles for sale or hire.

BUYING ONLINE... THE BASICS

Buying Online - The Basics

Always research to find out what a fair price is for similar goods; if the offer sounds too good to miss out on, it might not really exist.

Check the seller or buyer's review history and feedback from other reviewers.

Always use the site's recommended payment site. If you pay any other way than via a recommended payment site, you may not be able to recover your money. Where there's no recommended payment site, paying via credit card or known third party payment providers is preferable to direct bank transfers.

Make sure that the website you're buying from is genuine – and not a fake or copycat site – by typing in the address yourself. Fake addresses usually vary from authentic ones with just one or two incorrect letters.

The web address should begin with 'https://'; the 's' stands for 'secure'

How the scammers work

The most common scams occur on online auction sites, where criminals pose as sellers of popular items, such as mobile phones and cars. After the payment is made they disappear, leaving you with no goods.

Criminals also pose as buyers on auction sites, sending spoof emails as proof of payment transfer. The payment fails to materialise, but the goods have already been sent.

Warning signs

It can be difficult to spot a scammer among the vast majority of genuine buyers and sellers.

Scammers will lure you in with 'irresistible' bargain prices for popular items that don't really exist.

They'll try to pressurise you into not using secure recommended payment sites and to pay via a bank transfer.

Fraudsters may pressurise you to transfer payment or a holding deposit before you have seen the item(s) in person.

FRAUD... THE BASICS

Help and Advice

Age UK
Provides companionship, advice and support for millions of older adults.
0800 169 6565
www.ageuk.org.uk

Cyber Aware
Cyber Aware provides cyber security advice for small business and individuals.
www.ncsc.gov.uk/cyberaware

Get Safe Online
Get Safe Online is the UK's most popular source of easy-to-understand information about online safety.
www.getsafeonline.org

Reporting

Royal Mail Scam Mail Helpline
Support and advice if you've received items by post that you believe to be fraudulent.
0800 011 3466

Report a scam email
Forward suspicious emails to report@phishing.gov.uk

Report a scam text
Forward suspicious text messages for free by forwarding it to 7726.

Report a scam phone call
If you've lost money you can contact your bank & report to Police Scotland on 101.

STAY SCEPTICAL - STOP AND THINK - COULD THIS BE A SCAM

FRAUD... THE BASICS

North East Division Crime Reduction Team

Moray (Keith)
PC Richard Russell
Richard.russell@scotland.police.uk

Aberdeenshire (Stonehaven)
PC Mike Urquhart
Michael.urquhart@scotland.police.uk

Aberdeen City (Nigg)
PC Mark Irvine
Mark.irvine@scotland.police.uk

STAY SCEPTICAL - STOP AND THINK - COULD THIS BE A SCAM