PROTECT YOURSELF FROM SCAMS

YOU ARE MORE LIKELY TO BE THE VICTIM OF ONLINE FRAUD THAN ANY OTHER CRIME

THIS GUIDE IS HERE TO HELP YOU!

sure.community foundation

TYPES OF ONLINE FRAUD

Scams can include anything from identity fraud, online transactions, dating scams and more, all designed to fool us and take our money.

Anyone can be caught by this type of fraud. The criminals work hard to trick people into believing the scam is genuine. They will use any route to do this such as by phone, instant messaging, on the internet and by email.

Inheritance Fraud – The criminal tells you that you're in line to receive a huge inheritance, but you'll need to pay a fee to release the funds.

Romance Fraud - Amongst genuine online dating profiles are fake profiles set up by criminals, these often use photographs taken from innocent people's social media accounts. The criminals are masters at emotional manipulation – They are after your money, not your love!

Lottery Fraud – You're told you've won a prize in a lottery, but you'll need to pay the criminal an admin fee.

Blackmail Fraud – The criminal threatens to share indecent images of the victim with all their contacts unless they get paid not to. They may also threaten children with the same, if information regarding their parents' personal information is not shared.

West African Letter Fraud – The criminal asks for help moving a large sum of money from one country to another, promising to cut you in, but asks for a payment upfront first.

Work From Home Fraud – The criminal offers you to make easy money working from home, but you need to pay a fee in advance, for business leads, or a website. They then gain access to your computer.

Computer Software Service Fraud - Criminals may contact you claiming there are problems with your computer or account, and they can help you to solve them. They will then instruct you to download a 'remote access' tool, which gives the criminal access to everything on your computer, now and in the future.

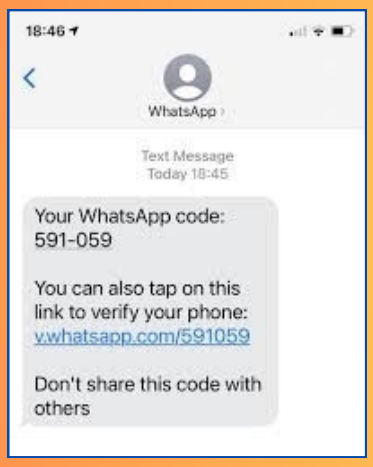
Holiday Fraud – The criminals will advertise flights, accommodation and other travel services that are not provided or don't exist. You probably won't find out until you try to travel.

Identity Fraud – Identity fraud involves the misuse of an individual's personal details to commit crime. Your details are valuable to criminals and can be misused by them or sold on to others.

Online shopping and auction sites – Among the genuine buyers and sellers, there are criminals who use well known internet sites to offer goods for sale they do not have or are fake.

Recovery Fraud – Once you've been a victim of fraud, the criminal contacts you, claiming that they can recover your losses, for a fee.

HOW DO ONLINE CRIMINALS FIND YOU?



There are several ways criminals can attack you and your device. They may search the internet to find insecure devices, send an email containing malicious software or may send an online message containing a fictitious WhatsApp code and ask you to click on a link.

Other ways criminals might get hold of your personal data:

Social Media and online forums – LinkedIn, Facebook, Twitter, Instagram, Reddit – all public platforms could hold a wealth of information about you.

Hacking and data breaches – Criminals can target organisations that store large amounts of data, like banks, email providers or online retailers. Once your personal details are leaked, they can be sold on the dark web.

Companies who sell your email address or phone number – always read terms and conditions when signing up for a product or service.

Hacking into email accounts - Ensure your IT systems are secure and be wary of using shared internet connections outside of work.

From you – You may give away reams of personal data if you participate in surveys, competitions and quizzes. This data can be sold to others legally or as part of a scam.

HOW TO SPOT SCAM MESSAGES OR CALLS

Scammers try to quickly gain your trust. They aim to pressure you into acting without thinking.

If a message or call makes you suspicious, stop, break the contact, and consider the language it uses. Scams often feature one or more of these tell-tale signs:

Authority - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.

Urgency - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.

Emotion - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

Scarcity - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

Current events - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year to make their scam seem more relevant to you.

HOW CAN YOU KEEP YOURSELF SAFE?

- Never send money to someone you have not met in person.
- Romance scammers lower the target's defences by building on online relationship, then play on your emotions eventually asking for larger and larger amounts of money. Be extremely wary of giving money to someone you have recently started a relationship with, regardless of the reasons they give. Talk to family and friends, or your bank, even if the person is asking to keep your relationship a secret. Well meaning men and women have both fallen victim to this.
- You cannot win a competition or lottery you have not entered! If you are asked to pay an upfront fee for such a 'win' do not pay!
- Be wary about the information you post online and ensure you check your privacy settings on social media sites.

If you receive an email or message from an unknown sender, ignore and block the number. **Never** click on links sent in these messages.

It's OK to reject, refuse or ignore requests for your personal or financial information. Only criminals will try to rush or panic you.

- Remember criminals will impersonate trusted organisations such as the NHS, the police and your bank. If you have any doubts about a message, contact the organisation directly. Don't use the numbers or address in the message – use the details from their official website.
- If a price seems too good to be true, then it may be a criminal taking advantage of our keenness to try and steal from us. Remember to avoid those who encourage/ push you to make payments outside of normal secure payment options.
- Have a strong and separate password for your email account.
- Never let anyone remotely access your computer.
- There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- Don't be persuaded to receive money into your account, no matter how plausible it seems. Money laundering is a crime that helps fund organised crime such as drugs, terrorism and human trafficking.

WHAT TO DO IF YOU GET SCAMMED

GET HELP AND REPORT A SCAM

If you think you have uncovered a scam, have been targeted by a scam or fallen victim, report this immediately to your bank and to the police on 28100.

REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target again.

The quicker you act, the more chance you have of reducing your losses.

Don't be afraid, but be aware. Don't be scared be sceptical. Always remember, if it sounds too good to be true it probably is!

Remember, if you have had money stolen online, **it is not your fault.** Scammers are professional criminals, highly trained experts in tricking their victims out of money.

WHERE TO ACCESS FURTHER SUPPORT

If you have been the victim of online fraud the following organisations may be able to offer additional support:

Sure South Atlantic maybe able to assist with increasing existing cyber security on your telephone and online devices.

The Emotional Wellbeing Service can offer support if you have become a victim of a scam. Call 28082 or email emotionalwellbeingservice@kemh.gov.fk

You can contact the **Samaritans** 24 hours a day, 7 days a week on 51515.

Social Services may also be contacted on 27296 or email referrals.social@kemh.gov.uk

The Citizens Advice Bureau can be contacted for advice on 55355 or email cab@horizon.co.fk

ADDITIONAL INFORMATION

Royal Falkland Islands Police
To report fraud, call RFIP on 28100 or email safe@police.gov.fk

Sure South Atlantic
Sure can provide advice and assistance with keeping yourself and your family safe online.

ACTION FRAUD
www.actionfraud.police.uk
Action Fraud provides a central point of contact for information about online fraud.

The Little Book of Big Scams
https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/the-little-book-of-big-scams.pdf
This book highlights the most common forms of online fraud and offers advice and guidance on how to protect yourself.

TAKE FIVE
www.takefive-stopfraud.org.uk
Take Five offers straight-forward, impartial advice that helps prevent email, phone-based and online fraud.

FRIENDS AGAINST SCAMS
www.friendsagainstscams.org.uk
Friends Against Scams is a website providing free information and training about scams and how to spot and report them.

CYBER AWARE
www.ncsc.gov.uk/cyberaware/home
Cyber Aware is the UK governments advice on how to stay secure online.

IMPORTANT THINGS TO REMEMBER

STOP

Taking a moment to think before parting with your money or information can keep you safe.

CHALLENGE

Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

ASK

If you're not sure, speak to someone you trust, such as family or bank staff before passing on any personal or financial information.

PROTECT

Contact your bank immediately if you think you are the victim of a scam and report it to RFIP on 28100.

sure.community foundation

Social Services Department

ROYAL FALKLAND ISLANDS POLICE