This information was provided by Devon and Cornwall Police on 24 June 2025, following an online information session hosted by Transformation Cornwall. While every effort has been made to ensure the accuracy of the content at the time of publication, some links or details may change over time. Users are therefore advised to verify any critical information independently where necessary.

TOP CYBER TIPS

1. USE STRONG PASSWORDS

- Consider using - **ThreeR@nd0mWord$** .
- Your password MUST contain at least 12 characters. Don't use the same password for all your accounts.
- The strongest should be for your primary email account and this password should not be used for anything else.
- Where possible activate 2 Factor Authentication (2FA) / Two-Step verification (2SV). This generally involves sending a text to your mobile phone to double check that it is you carrying out a particular transaction.
- If you have difficulties remembering lots of passwords, consider using an on-line *'password manager'*. There are various free and paid for *password managers* available, for example: KEEPER, NORDPASS, ROBOFORM, BITWARDEN, 1PASSWORD
- Consider saving passwords in your web browser, although not on a shared device.

2. UPDATES & APPS

- Always take operating system and software updates as soon as possible.
- Turn on your Anti-Virus / Firewall and keep them updated.
- Don't use old operating systems that are no longer supported. These are particularly vulnerable to attack.
- Only download Apps from accredited Apps stores.

3. BACK-UPS

- Regularly back-up your important data onto a removable hard drive.
- Consider keeping your back-ups off-site, in a fireproof / waterproof safe.

4. PHISHING / SOCIAL ENGINEERING

- Never assume incoming emails are genuine. Even if you recognise the email address because email accounts can be *'hacked'*.
- Never believe voice calls and text messages are genuine, even if you recognise the phone number. Phone numbers can be *'Spoofed'* (falsified).
- ALWAYS CONFIRM using the contact information you have obtained from your own records or from publicly available sources. Remember **–** Criminals will PHISH to obtain information from you.
- DON'T GIVE OUT ANY SENSITIVE INFORMATION TO INCOMING CALLERS.
- Send all email PHISHING attempts to **report@phishing.gov.uk .**
- Send **fake text messages onto 7726** (Spam).
- **Call 159** to quickly be directed to your **bank's Fraud Team.**

5. CHECK YOUR PRIVACY SETTINGS

- Regularly check the privacy settings on your Social Media accounts and be careful what you post on social media. Do you really want everyone to know your house is empty when you are away on holiday?

6. BE CAUTIOUS WHEN USING PUBLIC WI-FI

- Don't pass sensitive information, passwords, or bank account details over public Wi-Fi.

7. SECURE YOUR DEVICES

- Ensure all your devices including your mobile phone(s) are password or PIN protected - Keep them 'locked' when not in use.
- Use Fingerprint or facial recognition if available.
- Only grant remote access to your device (computer / mobile phone / tablet), to someone you personally know and thoroughly trust.
- Never grant remote access to any incoming telephone callers.
- Try and avoid using publicly available USB re-charging points. These can be interfered with to compromise the security of your device (*Juice Jacking*). It is generally safer to charge devices from a standard electricity point or your own portable powerpack.

8. CREDIT CARDS

- For added protection, please use a credit card for all your on-line transactions.

9. BE CAUTIOUS OF QR CODES

- Carefully check QR codes before scanning them. Do they look genuine? Have they been tampered with? Can you do the transaction without using the QR code? Avoid Scanning from unknown / untrusted sources

10. INCOMING MESSAGES

- Be wary of ALL incoming messages, including, voice calls, SMS text messages, emails and social media messages, even from people you may know or email addresses you recognise. Remember accounts can be hacked and emails, social media addresses and phone numbers can be *Spoofed* (falsified). Both voice calls and videos from individuals know personally can be 'DEEP FAKED'. Don't rely on caller ID display. If you are concerned about an incoming call, hang up, call the caller back using another phone and the phone number YOU have obtained yourself from your own trusted sources.
- Never Assume, Never Believe, Do not give personal details instead ALWAYS CONFIRM DETAILS. Be particularly cautious of any requests you may get to change the details of a regular outgoing payment or to create a new payment. Always think - IS THIS A PDF / Payment Diversion Fraud.

11. NEVER SHARE YOUR PASSWORDS

- Organisations including financial institutions, HMRC, the DVLA, the NHS, other Government bodies, and the Police will never ask for YOUR PIN, YOUR Passwords, YOUR personal / financial details. NEVER-EVER share those details. Any requests you get, claiming to come from such organisations WILL BE A SCAM!

12. SLOW DOWN – DON'T RUSH

- Question Everything / Seek Advice / Never Assume, Never Believe, ALWAYS CONFIRM.

REPORTING CYBER CRIME

Action Fraud customer channels

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Social Media
Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.

0300 123 2040
Report fraud and cyber crime.
Help, support and advice.

24/7 Live cyber
Specialist line for business, charities or organisations suffering live cyber attacks

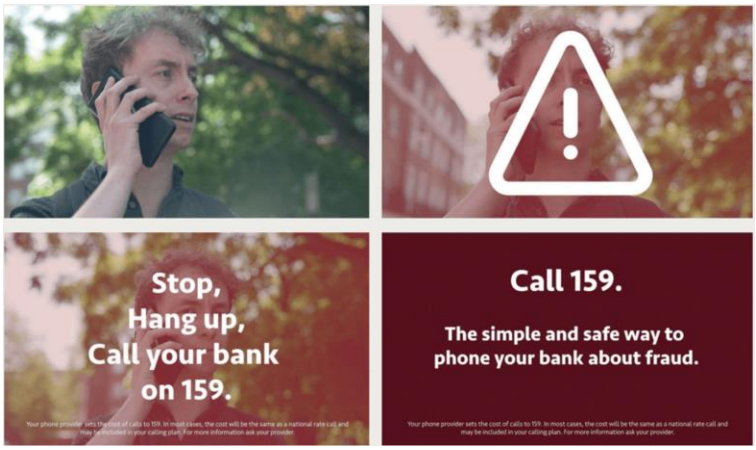
Report 24/7 & Web Chat
www.actionfraud.police.uk
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

WORRIED ABOUT FRAUD ON YOUR BANK ACCOUNT ?



STOP, HANG UP, CALL 159

If you receive a suspicious call, text, or email that appears to be from your bank or another trusted organisation, you should: Stop, hang up, and call 159.

This number connects you directly to **your bank's fraud prevention team**, bypassing any potential scammer who may still be on the line. Ideally, call 159 from a different phone line

USEFUL WEBSITES

Devon and Cornwall Police – Alert Service
A free, two-way community messaging system operated by Devon and Cornwall Police. It's designed to keep residents informed about what's happening in their local area and to encourage community engagement. To sign up to specific alerts go to : **Home Page - Devon and Cornwall Alert**

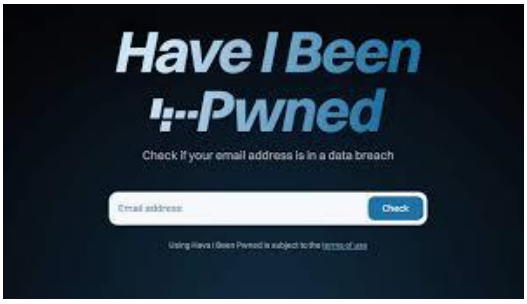
https://stopthinkfraud.campaign.gov.uk

Led by the UK Government's Home Office in collaboration with the National Cyber Security Centre (NCSC), City of London Police, and the National Crime Agency (NCA), this campaign aims to:

- Raise awareness of the impact of fraud.
- Empower the public with tools and knowledge to recognise and avoid scams.
- Disrupt fraudsters by working with industries to block scams before they reach people

https://www.ncsc.gov.uk/section/advice-guidance

The NCSC is the UK's 'technical authority' for cyber incidents. The NCSC website provides a range of practical cyber security advice to individuals, businesses, and public sector organisations



Check online if your email has been compromised in a databreach

Go to Have I Been Pwned

Take Five
Take Five - To Stop Fraud

A UK-wide awareness campaign led by UK Finance and supported by the government and various partners. Its goal is to help individuals and businesses protect themselves from financial fraud, especially scams involving impersonation of trusted organisations.

USEFUL CONTACT

Devon and Cornwall's Cyber Protect team can be contacted by email at: cyberprotect@devonandcornwall.pnn.police.uk