

Top Tips

1. **PASSWORDS** - Use Strong Passwords. Consider using – THREE RANDOM WORDS (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 email and financial accounts and this password should not be used for anything else.
- **Where possible activate 2 Factor Authentication (2FA) / Two-Step verification (2SV).**
- 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.
- Go to [Have I Been Pwned: Check if your email has been compromised in a data breach](https://haveibeenpwned.com/) (<https://haveibeenpwned.com/>) to see if your email has been involved in a data-breach.

2. **UPDATES and 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.**

- Always Back up your data
- In addition to Cloud Backups Consider Regularly backing up your important data onto a removable hard drive.
- Consider how to keep your backup 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 Messages.**
- Send all email PHISHING attempts to **Report FRAUD**
 - report@phishing.gov.uk
 - **Report and Block** all Phishing Emails , Text Messages and Calls
 - If you do not have the Report and Block feature available on your device, you can send fake text messages onto 7726 (Spam)

5. **PRIVACY SETTINGS.**

- Check the privacy settings on your Social Media accounts.
- Be careful what you post on social media, do not share and like from contacts you do not know

- Check you location and privacy settings on your devices
- Close and delete unused accounts

6. **WI-FI.**

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

7. **SECURING 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.

8. **INCOMING MESSAGES.**

- Be wary of **ALL** incoming messages, including, voice calls, SMS text messages, emails and social media messages
- Even from persons 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).
- If you are concerned about an incoming call, hang up, call or text the caller back using another phone and the phone number YOU have obtained yourself from your own trusted sources.
- Never Assume, Never Believe, **ALWAYS CONFIRM**.

9. **QR CODES.**

- Carefully check QR codes before scanning them. Do they look genuine? Have they been tampered with?
- Can you complete the transaction without using the QR code?
- Avoid Scanning from unknown / untrusted sources
- Never make payments to unverified QR Codes

10. **Never share your passwords.**

- Never Share Passwords
- Never Share One Time Passcodes
- 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

11. **SLOW DOWN (Don't Rush) & VERIFY**

- Never Act quickly
- Check with your friends and Family
- Question Everything / Seek Advice /
 - Never Assume,

- Never Believe,
- **ALWAYS CONFIRM.**

Community Messaging



The Service Previously known as Devon and Cornwall Alert is now called “Community Messaging” – Information and Sign Up can be found here - [Home Page – Community Messaging](#)

Reporting Cyber Crime

<https://reportfraud.police.uk>



0300 123 2040

Report fraud and cyber crime.
Help, support and advice.

Monday-Friday - 8am-8pm

Report 24/7 & Web Chat

UK's Home for Reporting
Cyber Crime & Fraud - Report Fraud

<https://www.reportfraud.police.uk>

Forward any **phishing emails** to - report@phishing.gov.uk

Forward the **suspicious text** to **7726**

Forward the **suspicious Calls** to **7726** - type "Call *number*"

Contact the Fraud Department of you bank – Dial 159

