Cyber Security…

Top Tips….

1. **PASSWORDS / 2FA / 2SV**. Use Strong Passwords (Remember - **ThreeR@nd0mWord$)** . Your password MUST contain at least 12 characters. Don't use the same password for all your accounts. 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. These include – KEEPER, NORDPASS, ROBOFORM, BITWARDEN, 1PASSWORD (please have a look at the latest reviews on-line). You can also consider saving passwords in your web browser

2. **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?

3. **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.

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

5. **WI-FI**. Be cautious when using public Wi-Fi and don't pass sensitive information over public Wi-Fi.

6. **SECURING YOUR DEVICE**. 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.

7. **PHISHING.** Remember **–** Criminals will PHISH to obtain information from you. Send all PHISHING attempts to **report@phishing.gov.uk**

8. **CREDIT CARDS**. Use a credit card for all your on-line transactions.

9. **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. Remember accounts can be hacked and emails, social media addresses and phone numbers can be spoofed. Don't rely on caller 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. Be particularly cautious of any requests you may get to change the details of a regular payment. Always think PDF / Payment Diversion Fraud.

10. **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?

11. **Organisations including financial institutions, HMRC and the Police will never ask for YOUR PIN, YOUR Passwords, YOUR personal / financial details. NEVER-EVER share those details.**

12. **Don't Rush / Question Everything / Seek Advice / Never Assume, Never Believe, ALWAYS CONFIRM. Take Five -** Take Five - To Stop Fraud | To Stop Fraud (takefive-stopfraud.org.uk)

Prepared by Mick Harrison, Devon & Cornwall Police.

mick.harrison@devonandcornwall.pnn.police.uk

April 2024.