Top Tips to Combat Fraud

1. **PASSWORDS / 2FA / 2SV**. 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. 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, although not on a shared device.

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**. 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** and send fake text messages onto 7726 (Spam). Call 159 to quickly be directed to your banks Fraud Team.

5. **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. **WI-FI**. Be cautious when using public Wi-Fi and 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. 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. **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?

10. **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). Both voice calls and videos from individuals you 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, ALWAYS CONFIRM. 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 or financial details. NEVER-EVER share those details. Any requests you get, claiming to come from such organisations WILL BE A SCAM!

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). Go to Have I Been Pwned: Check if your email has been compromised in a data breach to see if your email has been involved in a data-breach. REMEMBER – NEVER CLICK ON ANY LINKS, NEVER DOWNLOAD ANY FILES FROM EMAILS OR MESSAGES YOU ARE NOT 100% SURE ABOUT. IF IT IS **OUT OF THE BLUE, IT'S NOT FOR YOU.** DELETE IT.

Mick HARRISON

PSE 31015

Cyber Protect Officer

Devon and Cornwall Police