STAFFORDSHIRE
POLICE

Cyber Awareness Month - Top Tips Oct. 2021

1. **Passwords** - Choose, use and protect passwords carefully. **Use a different password for every online account, especially your email, this helps protect other accounts if one becomes compromised**. The longer a password is, the stronger it will be, so best advice is to use a minimum of **three random words.** Choose words wisely avoiding family, friends, pet names, sports clubs and commonly used phrases. You can add special characters and symbols, these will add extra strength to your passwords. NEVER DISCLOSE YOUR PASSWORD.

2. **Two-Factor Authentication (2FA)** - If a password is compromised by cyber criminals, it can potentially give them access to your online accounts. However, accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they will have difficulty accessing your account. 2FA provides a way of 'double checking' that you really **are** the person you are claiming to be when you're using online services, such as banking, email or social media. **It is available on most of the major online services and should be used wherever possible.**

3. **Antivirus (AV)** – To help protect your systems and devices against viruses and malware (malicious software), it is important to use **suitable antivirus** (internet security software). Most systems have this software built in so make sure it is switched on and kept updated as a minimum, you can add additional Antivirus if you wish. Remember that some smartphones and tablets can get compromised too, so ensure they are also protected.

4. **Update/Patch** – Updates improve user experience and importantly fix vulnerabilities ('holes') in software applications; if software isn't updated/patched this can allow unwanted 'bugs' in, so it is vital to **apply them as soon as possible** to ensure software and apps are better protected. Where possible, set systems to automated update.

5. **Back up Data** - The information held on devices may be irreplaceable. Regularly backing up your data will ensure that you have more than one copy; two principal methods are the use of 'online (cloud) storage', or 'portable hard drives' (can be stored off site for additional security).

6. **Phishing - Clicking Links** – Be vigilant to links in emails, social media messages, posts, tweets and texts which could be malicious and avoid automatically opening attachments – if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving it, it could be phishing in attempt to distribute malware or obtain personal and/or financial information. **Stop Challenge and Verify** via a known and trusted source and never respond to a sender you are suspicious of.

7. **Protect Your Identity** – Be mindful as to how much **personal or financial information you share -** in emails, on social networking and dating sites, even in person. You never know if it may become compromised and who might see it, or use it.

8. **Is this person genuine?** - Always consider that either online or on the phone, people aren't always who they claim to be. In addition to phishing emails, phone numbers can be spoofed (faked) and fraudulent phone calls are a favourite way for fraudsters to approach their victims.

9. **Shopping Online** – When making purchases online, research the seller well, are they genuine? Is an offer too good to be true? Have you done business with them before? Choose safer methods to pay, for example pay with a credit card. **Payments** - It is better to avoid paying for anything by direct bank transfer – including goods, services, tickets, travel and holidays – unless it is to someone you know personally, is reputable and the destination account is correct and can be verified.

10. **Public Wi-Fi** - Wi-Fi hotspots in places like cafes, bars and hotel rooms can be insecure, so it is better to avoid the use of them when you're doing anything confidential online – logging into accounts using passwords, emails, sending and receiving messages, shopping, working. Instead, use 3G, 4G or 5G, or use a VPN (virtual private network).

TAKE FIVE – if you are unsure or suspicious, STOP, THINK and remember:

Being tempted, pressured, rushed? It's okay to seek advice from someone you trust

TAKE FIVE TO STOP FRAUD

Visit the National Cyber Security Centre (NCSC) website for additional cyber security advice:
https://www.ncsc.gov.uk/cyberaware/home

Report cyber-crime and fraud to Action Fraud:

actionfraud.police.uk

Businesses suffering a live cyber-attack can contact Action Fraud 24/7 for support, call:

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Received a phishing email?

Forward suspicious emails to: report@phishing.gov.uk

Received a suspicious text message?

You can report fraudulent texts by forwarding to: **7726**

Suspicious website?

You can report a suspicious website to:

https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

For Local Cyber Awareness Sessions & Events, contact the Cyber Crime Unit at:
CyberCrimeUnit@staffordshire.pnn.police.uk