STAFFORDSHIRE POLICE

Cyber Champion Tips – April 2021

Revisiting Passwords

Strong passwords are one of the **Cyber Aware** campaign's six top tips for cyber security, so this month we will look at the importance of using strong passwords to protect online accounts. Why? Well strong passwords are a hugely important factor for good cyber hygiene and are significant in preventing unauthorised access to online accounts and devices. Unauthorised access, or unethical hacks, can be a real headache and can cause numerous issues, some of which can be very tricky to resolve.

In this ever-increasing world of online activity, one of the most important things you can do, is get into the habit of using strong passwords. Consider your passwords like you treat the security of your home. Exterior doors need to be strong and robust, the more security features your front door has, frame, door type, locking mechanism, etc., the harder it is for a criminal to get through it; the same applies for passwords, the stronger your password, the more secure your online accounts and devices will be.

So how do we create a strong password?

1/ **Use three random words** - avoid the use of family/friends/pet names, these are easier guessed due to availability of information shared on social media platforms. Choose words which are random only to you.

2/ **Length** – Try to choose longer words, the longer the password is, the stronger it will be. Passwords which are complex may seem strong, but if they are not of suitable character length, they are vulnerable to attack.

Here are examples of both poor and strong passwords:

Poor password examples:

- football
- 654321
- Admin222
- w>xL&4@k

✗

Strong password examples:

- cakescupboardsdelightful
- bookcaseangelsausages

And if you need to include symbols, numbers, get creative like this:

'buildingmonkeyglasses'

could be:

'8uildingmonKeygla$$e5

✓

It is important to note that the password examples used here are for demonstration purposes only and should not be used for actual accounts or devices.

3/ The next important tip for passwords, is to **use different passwords** for different accounts and devices. At the very least, make sure your email password is different from any others. Many people use the same passwords for everything, but this leaves them vulnerable to attack. Simply put, having the same password is like having a master key to a building in the physical world, with a master key, you can access all locked areas; the same applies to passwords, if one account is compromised, so are the rest.

A Multi-layered Approach - Hopefully that helps to reinforce the importance of passwords, but passwords are only part of a good security solution, for good cyber security practices to work at their best, a multi-layered approach is a must. A great foundation in applying a multilayered approach to boost your cyber security is to use strong passwords alongside the security measures featured in the National Cyber Security Centre's (NCSC) **Cyber Aware** campaign, you can find out more about the six security measures featured in the campaign here: https://www.ncsc.gov.uk/cyberaware/home

Current News

All Businesses & Organisations - Introducing Police CyberAlarm - Free tool to help improve cyber resilience

We are pleased to announce that every business and organisation in the region can now get access to a free tool called Police CyberAlarm, designed to help them understand and monitor the threats they face from malicious cyber activity.

Funded by Government, Police CyberAlarm acts as like 'CCTV camera' monitoring the traffic seen by a businesses' connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling a business to take steps to improve their cyber resilience. A Police CyberAlarm member will benefit from regular reports detailing suspicious and potentially malicious attack activity on their firewall/ internet gateway. It will show them how they are being attacked, and where from so they can improve their cyber resilience. It will also help law enforcement identify current threats and take enforcement action against cyber criminals.

Find out more and how you can sign up here: https://cyberalarm.police.uk/

Community - Be Vigilant to Fake Event/Festival Tickets Online

As we come into spring and tentatively venture out of lockdown, there will be lots of activity and excitement as we are able to book events, festivals and breaks away. With this in mind, there will be unscrupulous cyber criminals looking to exploit this increased activity, the National Fraud Intelligence Bureau (NFIB) are warning people to extra vigilant when buying tickets online due to fraudsters selling fake or non-existent tickets to events.

Action Fraud have issued the following advice for anybody purchasing tickets:

- 'Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal offer greater protection against fraud.

- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

Action Fraud'

Education Sector - Ransomware Attacks, a Continuing Threat

'The NCSC continues to respond to an increased number of ransomware attacks affecting education establishments in the UK, including schools, colleges, and universities.

Since late February 2021, an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities. The NCSC previously acknowledged an increase in ransomware attacks on the UK education sector during August and September 2020.

Advice and Support - The NCSC urges all organisations to follow their guidance on 'Mitigating Malware and Ransomware', which details a number of steps organisations can take to disrupt ransomware attack vectors and enable effective recovery from ransomware attacks:

https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

Education Sector - NCSC School Staff Training – Free cyber security training resource

SCHOOLS will be able to improve their defence against online attacks through new training created for teachers and staff by the UK's leading cyber experts. The National Cyber Security Centre has released free cyber security training for school staff, the training sets out real-life incident case studies and four practical steps staff can take to protect themselves online and help boost cyber resilience which can help mitigate cyber incidents, including ransomware attacks. Find out more information and access to the training here: https://www.ncsc.gov.uk/information/cyber-security-training-schools

March & April NCSC threat reports here:

26th March 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-26th-march-2021

- Microsoft Exchange Server vulnerabilities
- 2021 survey reveals cyber risks to UK organisations
- Decline in students learning digital skills
- NCSC warns education sector of rise in cyber attacks

2nd April 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-2nd-april-2021

- Education continues to face ransomware threat
- CEOs identify cyber security as an ongoing concern

12th April 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-12th-april-2021

- Spoof job offer for LinkedIn users
- Facebook user data leaked online
- Fresh warning over risks to unpatched Fortinet VPN devices

16th April 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-16th-april-2021

- DNS vulnerabilities could impact millions of devices worldwide
- NCSC recommends organisations install critical Microsoft Exchange updates
- UK and US call out Russia for SolarWinds compromise

23rd April 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-23rd-april-2021

- FluBot "package delivery" scam targeting Android devices
- Pulse Connect Secure RCE Vulnerability
- University IT systems still offline due to cyber attack

30th April 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-30th-april-2021

- Hackers threaten to leak confidential US police data
- Hedge funds warned of complex scams

West Midlands Regional Cyber Crime Unit (WMRCCU): Take a visit to the WMRCCU website where you will find current information, advice, podcasts and subscription to the **Cyber Crime Sentinel**, check it out here: https://www.wmcyber.org/

Reporting

Report cyber-crime and fraud to Action Fraud:
actionfraud.police.uk

Businesses suffering a live cyber-attack can call: 0300 123 2040

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**

If a scam text claims to be from your bank, you should also report it to them

Further advice can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

takefive-stopfraud.org.uk

ukfinance.org.uk

staffordshire.police.uk

TAKE FIVE
TO STOP FRAUD