STAFFORDSHIRE POLICE

Cyber Champions Tips June 2020

It is a known fact that criminals will adapt and use current trends and themes to tailor attacks. It comes as no surprise then that criminals are taking advantage of the **NHS Test and Trace service** in attempt to get people to part with their personal and financial details. Here is some great advice:

NHS Test and Trace

Criminals are sending phishing emails and texts containing links designed to obtain banking passwords and PINs, there is also the risk posed by fraudulent callers.

If you receive a suspicious text, email or phone call, make sure you Stop Challenge Protect.

Ensure you check web addresses very carefully and avoid clicking on links. Always use a safe source, for example typing the official address directly into your browser. It's important to remember that NHS Test and Trace will never ask for money, financial details, PINs or passwords and they will never visit your home.

The official NHS Test and Trace website address is: https://contact-tracing.phe.gov.uk

Further information on NHS Test and Trace can be found by visiting the GOV.UK website here: https://www.gov.uk/guidance/nhs-test-and-trace-how-it-works

And further information from Action Fraud here: https://www.actionfraud.police.uk/testandtrace

Reporting

Been subject to cyber-crime or fraud?

Always report this to Action Fraud here: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

*** Action Fraud have 24 hours support for businesses suffering a live cyber-attack, in this event please call 0300 123 2040 ***

Received a phishing email?

Forward the original email to the **Suspicious Email Reporting Service (SERS),** an automated system will scan the email and if malicious links are found, the associated website will be taken down:

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.

Resources

With the increased connectivity during recent weeks, it's a really good opportunity to check if your cyber practices and behaviours are still protecting you, your family and your business. There are some fantastic resources out there offering great cyber security tips and advice, no more so than those provided by the National Cyber Security Centre (NCSC). The NCSC provide all sorts of information for business and the wider public from their 'Board Room Toolkit and Top Tips for Staff' and their new campaign **Cyber Aware** with the 'Six Top Tips' to support everyone:

CyberAware.gov.uk

NCSC's free ELearning and Top Tips for Staff

Perhaps revisit the eLearning for staff, it's free and only takes about 30 minutes, so well worth a go for the team:

https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

NCSC 's Exercise in a Box

What about Exercise in a Box? 'Exercise in a Box is an online tool from the NCSC which helps organisations test and practise their response to a cyber attack. It is completely free and you don't have to be an expert to use it.

The service provides exercises, based around the main cyber threats, which your organisation can do in your own time, in a safe environment, as many times as you want. It includes everything you need for setting up, planning, delivery, and post-exercise activity, all in one place, if you want to see how well prepared your business is, it may be worth getting the team together and having a go' *NCSC*. So just how prepared are you? Why not have a go, check it out with your team here:

https://www.ncsc.gov.uk/information/exercise-in-a-box

News

Football Returns - The NCSC is urging football fans to secure their online platform streaming accounts and subscriptions as scores of fans are expected to log on and stream during behind closed door games. The NCSC has previously revealed that almost 700,000 accounts have been compromised through hackers guessing a device's passwords as 'liverpool', 'chelsea' or 'arsenal' *NCSC*. Check out the full article here: https://www.actionfraud.police.uk/news/avoid-scoring-a-cyber-own-goal-when-streaming-premier-leagues-return

Strong passwords – Three random words

Online Shopping Losses totalling £16.1million – Online shopping scams are increasingly prevalent as more people are shopping and buying goods online, people have ordered items such as hand sanitiser, face masks and gloves which have never arrived, and when they have, they have been sub-standard. Other items including vehicles, people paying deposits for vehicles which don't exist or materialise, technology, electronics, etc. Action Fraud report: 'Since shops were forced to close due to the coronavirus outbreak on 23 March, Action Fraud has received reports of online shopping fraud totalling £16.6million* in losses. Members of the public have reported buying mobile phones (19%), vehicles (22%), electronics (10%) such as games consoles, AirPods and MacBooks , and footwear (4%) on sites such as eBay (18%), Facebook (18%), Gumtree (10%) and Depop (6%)' *Action Fraud*. It pays to check sellers carefully. Have they got good feedback? Have they sold before? Check to see if the seller is genuine. Always try to purchase goods from trusted sources where possible and ensure any payments are protected, avoid paying by bank transfer which offers little protection if you become a victim of fraud. Instead, use a credit card or a payment service such as PayPal. https://www.actionfraud.police.uk/alert/over-16-million-lost-to-online-shopping-fraud-during-lockdown-with-people-aged-18-26-most-at-risk

Awareness videos:

We have been busy producing several short videos to get awareness messages out during Covid-19 restrictions, here are links to the videos which you can view, we are also happy for you to download and share via your networks, platforms and communities as you see fit. Prevention? Education is key:

Stay Safe. Stop Scams. Be Secure.

Phishing: https://vimeo.com/staffspolice/phishing

Cyber Aware: https://vimeo.com/staffspolice/cyber-aware

Smishing: https://vimeo.com/staffspolice/smishing

Vishing (voice solicitation): https://vimeo.com/staffspolice/vishing

Scam Alert: https://vimeo.com/staffspolice/scam-alert

We have also produced the videos in British Sign Language for the dDeaf community - dDeaf 'dD' is the term used to describe individuals who are Deaf (sign language users) and deaf (who are hard of hearing but have English as their first language and may lip read and or use hearing aids.

BSL Phishing: https://vimeo.com/staffspolice/bsl-phishing

BSL Cyber Aware: https://vimeo.com/staffspolice/bsl-cyber-aware

BSL Smishing: https://vimeo.com/staffspolice/bsl-smishing

BSL Scam Alert: https://vimeo.com/staffspolice/bsl-scam-alert

Further information can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

Takefive-stopfraud.org.uk

Staffordshire.police.uk