Cyber Champions Tips

December 2020

News and Latest Scams

Spoofing numbers and Vishing (fraudulent) calls: We need to continue to be vigilant to fraudulent phone calls and the use of spoofed numbers, our own force back up number '0300 123 4455', was spoofed earlier this month. **Advice - never** trust caller display as number can be fake and **never** disclose personal or financial details to anyone you do not know and trust. Have the confidence to STOP and CHALLENGE to PROTECT your personal information and safeguard your money.

Postal Delivery Issues: '**UK Finance warns public to beware of parcel delivery scams in run up to Christmas.** Intelligence from UK Finance suggests that criminals are sending out phishing emails, purportedly from well-known delivery companies, which claim that they have been unable to deliver parcels, packages or large letters. **The public should also be aware of an increased risk of scam phone calls and texts impersonating delivery companies, as well as fake delivery notices posted through letterboxes.** *UK Finance*

Further from Action Fraud……….

242K Lost to Fake DPD Emails and Texts: '**In November alone, the Suspicious Email Reporting Service SERS), received 5,478 reports of suspicious DPD emails**. This is an increase of 655% when compared to the previous month. Action Fraud has also received 166 reports of suspicious DPD text messages between June and November this year, with victims reporting a total loss of £139,000. A further 35 reports were made in the first week of December, with victims reporting a total loss of £103,000.

The messages purporting to be from DPD claims that the delivery driver was "unable to deliver your parcel today" as "you weren't in or there was no safe place to leave it". The message provides instructions on how arrange another delivery. The links in the messages lead to fraudulent websites that request a small payment to rearrange the delivery. If the victim makes this payment, they'll receive a phone call within a few days from someone purporting to be from their bank to inform them about suspicious transactions on their account. Criminals carrying out this scam are able to use a tactic called 'spoofing' to make the call or text appear genuine by cloning the phone number, or sender ID, used by the bank'. *Action Fraud*

General Crime Prevention for deliveries: If you are expecting a parcel, try to arrange suitable, safe delivery, don't advertise to burglars that you may be out by putting notices on doors or windows which may highlight the property is unoccupied.

2.1 Million Lost in One Month to Tech Support Scams: '2,007 reports of computer software fraud were made to Action Fraud last month. Victims reported losing a total of £2,148,976. This is a 22% increase in reporting compared to the previous month.

Action Fraud has received reports of criminals cold calling victims purporting to be calling from well-known broadband providers primarily, claiming that the victim has a problem with their computer, router or internet. The suspect persuades the victim to download and connect via a Remote Access Tool (RAT), allowing the suspect to gain access to the victim's computer or mobile phone. Some reports also state that criminals have been using browser pop up windows to initiate contact with victims. Victims are then persuaded to log into their online banking to receive a refund from the broadband provider as a form of compensation. This allows the suspect access to the victim's bank account, and the ability to move funds out of the victims account into a UK mule account.

There has also been an increase in the variety of service providers being impersonated, with multiple providers being affected.' *Action Fraud*

TAKE FIVE to STOP – CHALLENGE – PROTECT

December NCSC threat reports here:

4th December 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-4th-december-2020

- Ransomware disrupts Maryland students
- Phishing attacks focus on online shoppers

11th December 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-11th-december-2020

- NSA urging VMWare patch action
- Leading cyber security firm reports attacks

18th December 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-18th-december-2020

- Guidance issued as SolarWinds compromised
- **Spotify** reset passwords following data breach

West Midlands Regional Cyber Crime Unit (WMRCCU):

The WMRCCU website has a host of information to help boost your cyber awareness and help keep you informed, take a visit where you will find tips, information and advice, check it out here: https://www.wmcyber.org/

Reporting

Been subject to cyber-crime or fraud?

Report to Action Fraud: actionfraud.police.uk

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

ActionFraud
National Fraud & Cyber Crime Reporting Centre
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.

Further information can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

takefive-stopfraud.org.uk

ukfinance.org.uk

Staffordshire.police.uk