East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 30 April 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is Virtual Private Networks

VPN stands for "**Virtual Private Network**," a term used to describe a digital network within another physical computer network. VPNs allow users to securely access protected information stored on a private network, using a public network.

VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and your services.

Protecting data in transit is one of the most important security aspects to consider when using mobile devices. Attackers with access to unprotected data (or inadequately-protected data) may be able to intercept and modify data, potentially causing harm.

Only traffic routed over the VPN will be protected, the VPN must establish a connection, remain connected while the device is in use, and reconnect if the connection is temporarily lost. To maintain security all traffic should be routed via the VPN.

Some operating systems and many third-party applications allow organisations to configure only certain applications to use a VPN on a device.

This is useful in a Bring Your Own Device (BYOD) scenario, where organisations do not want network traffic from personal apps to traverse the corporate network.

Details of how to choose and configure a VPN can be found on the NCSC website here

Charitable causes

Special mention today for Captain Tom Moore, achieving so many milestones.

- 100 years old today
- Raising over **£30 million** for NHS charities
- Promotion to "Colonel"

While we congratulate Tom on his fundraising efforts let's also be aware that fraudsters may create fake websites and steal donations from worthy causes, always check if the cause is genuine and the website is genuine.

Hot topics

No free beer! - Heineken said in a statement: "Please be aware that there is currently a 'free beer' phishing scam circulating through social networks. "The promotion states that

Heineken is giving away free kegs and encourages recipients to share the message. "This is a scam and is not sanctioned by Heineken.

Malicious emails are being circulated in relation to HMRC tax returns claims around COVID 19. This is being sent via email and when the user clicks on the link it is diverted to a fake website that asks for details. These websites have domain names that may have HMRC in the name but are fake websites, to access the HMRC website always go via www.gov.uk.

In the last 24 hours, there have been losses of £72,154 reported from people who have purchased large quantities of face masks online which have not been delivered.

Email purporting to be from the government, which states the victim has been fined £77 for leaving their home yesterday. The email provides a link and encourages the victim to click it to find out more.

These frequently reported scams have all been highlighted before but worth a reminder:

- Suspect calling purporting to be victim's bank, saying account was compromised/there had been unusual activity. Victim advised to open new account/transfer money there and then. Victim told they should not visit their branch because of COVID-19.
- Victim is persuaded by the suspect to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property. The property does not exist.
- Suspect advertises a pet online (puppy or kitten) and uses the outbreak as a reason the victim can't come and see the animal. The suspect sends photos and persuades the victim to make payment in advance. The suspect never provides the pet.
- Victim tried to apply for a government grant to assist their business during the outbreak but was informed their business had already received a grant and were therefore not eligible for any more financial assistance. The victim did not make this initial application and does not recognise the account the payment was made to.
- Victim receives a call purporting to be from the NHS (SHIELD or another COVID-19 department). Suspect attempts to get personal details over the phone.

Webinar - Monday 4th May 2020 @ 1400 – 1500 hrs

This week's topic: **The Internet of Things – Protecting your devices, data, and home.**

Internet of Things (IoT) devices feature in many homes, but are also increasingly integrated into industry infrastructures. This session, and the themes covered are applicable to both individuals and businesses.

SW Regional Cyber Crime Unit will take you through a real life cybercrime investigation involving internet connected devices and the challenges that law enforcement faced to bring an offender to justice

To register for this event click on the following link - places are limited.

All webinar series from the National Policing Cyber Protect Network will be available here

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.