East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 20 May 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 (VPNs)

Tunnels have been used to secretly move information and people for hundreds of years. Hidden from view, numerous tunnels were used to transport refugees, spies and information under the Berlin wall.

A VPN, is an encrypted connection over the Internet from a device to a network, encryption prevents electronic eavesdropping by scrambling the data so that it is unreadable whilst in transit; a 'tunnel' across the public internet, hiding data from prying eyes.

Remote access VPNs securely connect devices, known as endpoints and may be laptops, tablets, or smartphones to an organisations network, across the internet. Advances in VPN technology allow security checks to be conducted on endpoints to make sure they meet certain criteria before connecting. The encrypted connection prevents unauthorised people from eavesdropping on the traffic and allows the user to conduct work remotely.

Site-to-site VPNs are used when distance makes it impractical to have direct network connections between different office/site locations. Dedicated equipment is used to establish and maintain a secure encrypted connection.

A personal VPN is a piece of software that can be downloaded and installed on a smartphone, tablet or laptop. When online, every device is assigned an IP address, this address can be used to trace a user's geographic location. The Internet Service Provider (ISP), the search engine used and websites visited, can all record browsing history. This can reveal all sorts of private information. A personal VPN will encrypt data and aims to hide a user's IP address and browsing history from third parties.

Public Wi-Fi is everywhere, connecting to the internet at a conference centre, hotel, business premises, on trains and buses or the local coffee shop. These are all insecure connections and any information travelling over the internet is not private unless encrypted.

With the growth in remote working many organisations will be looking at the advantages of deploying VPN technology; enabling legacy systems to work remotely, protecting internal network servers by limiting access to authenticated devices, forcing traffic between a device and external services through internal, protective monitoring tools, and monitoring and/or filtering of users' network traffic.

Further more detailed advice from the NCSC can be found here

East Midlands Special Operations Unit

Hot topics

EasyJet confirmed that it has suffered a cyber-attack and is in the process of contacting affected customers following the incident.

The NCSC would recommend anybody with accounts that could have been compromised to be especially vigilant against any unusual activity in their bank accounts or suspicious phone calls and emails asking them for further information. Consider changing passwords for accounts that may have been affected. More information can be here.

Vehicle for sale scam (usually a campervan) in which the victim is not allowed to view the vehicle, and arranges for it to be delivered. Victims are given the option of paying by bank transfer or through PayPal, but the PayPal link is a spoofed site. The vehicle is never delivered.

Phishing emails sent from the email address HMRC@hotmail.com, offering a grant of £2,500 to £7,500 to tax payers out of work or working less because of the pandemic. The recipient is told to click on a link to check their eligibility.

Emails targeting outlook email account holders, the subject line reads Covid-19 Account Upgrade. The email claims that due to the outbreak, previous versions of outlook are being closed on May 12th and instructs recipients to follow a link to update their account.

Scams using fake celebrity endorsements for Covid-19 related giveaways have grown, on the back of authentic offers of cash etc from real celebrities; making it all the more difficult for fans to decide what is real and what is a scam.

Emails purporting to be from an online marketing millionaire offering short-term, online employment to people in financial difficulty because of the pandemic. The email offers cash for an undefined role and links to a spam site. Another email targets students and offers money for watching YouTube videos. This email contains four links to a malware site.

Webinar – Thursday 21st May 2020 @ 1400 – 1500 hrs

Topic: Out with the old, in with the new - A perspective from the next generation.

Are you bored of listening to the current world of Cyber Security specialists telling you what the industry and next generation needs?

Do you want to hear from the next generation themselves?

The City of London Police's Cyber Griffin team are excited to partner with CyberFirst, Tesco and Cygenta to bring you this opportunity. During this free one hour webinar, Dr. Jessica Barker will be speaking to four CyberFirst students, bringing you a truly unique perspective on the future of cyber security.

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

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.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).