East Midlands Special Operations Unit

CYBER AND FRAUD PROTECT WEEKLY SECURITY ARTICLE

Thursday 7 January 2021

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

If you require any further information, assistance or guidance please contact EMSOU Protect Team

Hot Topic: COVID-19 vaccination phishing SMS text message

There has been an increasing trend of COVID-19 phishing and SMS text message scams, prompting the NCSC to publish materials to raise awareness (see attached leaflet).

As it stands, there are five key trends:

- Fake URL links claiming to redirect you to GOV.UK website to claim relief payments.
- Lockdown fines suggesting you have breached government regulations.
- Offers of health supplements that will prevent you from being infected.
- Financial support that appears to be from your bank.
- Fake text messages claiming to be from the NHS advising individuals that they are eligible to apply for vaccine, but requiring sensitive data such as financial information to make a payment.

To protect yourself and those close to you:

- **Keep abreast of the news:** As awful as it may seem, knowledge of attack methods and techniques will hone the ability to separate fact from fiction.
- **Never click links within emails or text messages:** Links take you to fake websites.
- **Never call back using an unrecognised SMS phone number:** This could lead you to speaking directly with a criminal or criminal organisation.
- **Use official channels:** For example, use GOV.UK to find relevant information about COVID support and support services. Once the official communication channels are known you can verify information and find out what the next steps are.
- **Guard your data:** A legitimate organisation won't make unsolicited requests for sensitive information or payments. For example, the vaccine is only available on the NHS for free to people in priority groups. Use the official NHS app only available from Google Play or Apple Store for more.
- **Don't give into pressure**: If someone tries to coerce you into giving them sensitive information, end the conversation.
- **Watch your digital footprint.** Cyber criminals will use social media accounts and relevant websites to research you and make their scams more effective. Request the removal of unnecessary information and check your privacy settings for every account.

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).