East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 15 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.**

Reliable sources of information are: National Cyber Security Centre (NCSC), Action Fraud and your regional/force Protect and Communications teams.

Latest NCSC scam advice

There is evidence of cyber criminals using a range of online techniques to trick people into handing over money or reveal sensitive information.

Criminals rely on social engineering methods, taking advantage of human traits such as curiosity and concern in order to persuade them to:

- Click on a link that may lead to a phishing website.
- Download an app containing malware or ransomware
- Open a file (such as an email attachment) which contains malware.

Any of the above could result in personal and financial data being stolen.

Advice - Never click on a link in an unsolicited email.

It's not just online that criminals will try to take advantage of people and the government has issued plenty of other useful advice to help prevent common scams:

- **Stop**: Take a moment to stop and think before parting with your money or information.
- **Challenge**: Could it be fake? It's ok to reject, refuse or ignore any requests.
- **Protect**: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

East Midlands Special Operations Unit

Hot Topics

Over 100 reports were sent to the National Fraud Intelligence Bureau (NFIB) of phishing emails claiming to be from TV Licencing between 10-13 April 2020. It is believed that they are attempting to steal the recipient's personal and financial details through a fraudulent link.

Latest examples of COVID19 related phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency

A COVID-19 variation on the 'Nigerian Prince' scam has been discovered in which digital fraudsters impersonated the U.S. Department of Treasury. Victims are being told to release all unclaimed ATM cards to curtail the recession because of the virus outbreak, for a $50 upfront fee. Although this is an American report, it may be seen within the UK in the future.

There have been recent incidents where victims have received an email threatening them with releasing a compromising video of them at their computer unless they send $3500 worth of bitcoin. Some of the intended victims didn't even have web cams! It would appear to be a randomly targeted email.

A data breach occurred of an individual working in payroll services for a company who pay over 200 workers. The individual was working from home due to the outbreak, and both their mobile phone and laptop were potentially compromised as the two were connected at the time.

Top tip – always have your device software and anti-virus software up to date.
Reports also received of website offering COVID-19 antibody blood tests.

Cyber criminals recently exploited the move to working from home during the lockdown. As less security checks were being made the fraudsters were able to hack a senior employee's business email address and persuade the accounts department to redirect payments to accounts they controlled.

Reporting

Reporting is CRUCIAL. Please report all Fraud and Cybercrime to Action Fraud either online or by calling 0300 123 2040.