East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 21 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 fraud

In the last few months we have seen a rise in the number of frauds and scams leveraging COVID-19.

Common scams targeting businesses include:

Government grant/tax refund scams – Government imposters contact businesses by email, phone or text suggesting they might qualify for a special COVID-19 government grant or a tax refund. Variations involve contacts through social media posts and messages.

Invoice/mandate scams – Criminals claiming to be from a regular supplier contact businesses and state their bank details have changed and ask to change payment details.

CEO impersonation scams – An employee receives a call or email from someone claiming to be a senior member of staff – they ask for urgent payment to a new account and create a sense of panic. Scammers may use spoofing software to appear genuine.

Tech support scams – With more people working remotely, criminals may impersonate well-known companies and offer to repair devices, trying to gain computer access or steal passwords and login details.

To avoid becoming a victim, businesses should;

- Be cautious about unexpected urgent communications offering financial assistance.
- Check that the information is genuine by using official government websites.
- Never rush a payment. Use contact details you have used before to check it is genuine.
- Be cautious about unexpected urgent requests for payment

Scams targeting customers also undermine businesses, criminals often impersonate businesses to defraud their customers, causing reputational damage and loss of business.

Common scams targeting individuals include:

Online shopping scams - During the lockdown there has been an increase in online shopping activity and fraudsters are keen to exploit this. Scammers are asking victims to pay deposits, or in full, for goods by bank transfer. Items such as protective face masks, hand sanitiser, COVID-19 testing kits, puppies, kittens, phones, household goods and gym equipment have all been offered for sale. Once paid, the scammers break off contact and the items never arrive or, as with protective masks, are sub-standard.

East Midlands Special Operations Unit

Direct payment by bank transfer does not provide the security, and dispute resolution, offered by some online market places and services such as PayPal.

Advanced payment fraud – The victim is persuaded to make an advance payment for a rental property. The suspect uses the COVID-19 outbreak as the reason the victim cannot view the non-existent property.

Push payment frauds - Suspects are incorporating the coronavirus pandemic into push payment frauds, using the outbreak to convince victims to speak with the suspect on the phone, saying the banks are closed etc.

Courier fraud - Fraudsters contact victims by telephone purporting to be a police officer or bank official. After some trust has been established, the fraudster will suggest; money has been removed from the victim's bank account and staff at the local bank branch are responsible or suspects have been arrested but the 'police' need money for evidence.

Victims are asked to go to their bank and withdraw money, foreign currency from an exchange or purchase an expensive item. This will be handed over to a courier for examination who will also be a fraudster. The victims are promised they will be reimbursed but in there is no further contact and the money is never seen again.

Fake bank letters - These convincing letters are a replica template from banks and include bank logo, address and signature from a customer service representative. The letters tell recipients that there have been some "unusual transactions" on their personal account or an outstanding payment that needs paying immediately and asks them to call a number highlighted in bold to confirm they are genuine.

When victims call, an automated welcome message is played and the caller asked to enter their card number, account number and sort code followed by their date of birth.

Webinar – Thursday 28st May 2020 @ 1400 – 1500 hrs

Join East Midlands Special Operations Unit, for a free Webinar on how to identify, respond and recover from cyber-attacks.

About this Event

The faster your organisation can detect and respond to a security incident, the less likely to have a significant impact on your data, reputation and finances. This presentation will help Business leaders and IT managers prepare for and respond effectively in a crisis.

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).