East Midlands Special Operations Unit

# COVID-19 CYBER AND FRAUD PROTECT MESSAGES

*Friday 05 June 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 'scams and fake news'

Mainstream media continue to report that false information is still a major concern during the coronavirus outbreak. A recent report from the BBC describes doctors and paramedics dealing with elements of misinformation on social media that COVID-19 was a mild illness, or remedies such as gargling salt water would help.

Trading Standards are seeking to halt sales of a device (a USB key costing £339.60) that claims to offer protection against the supposed dangers of 5G; *"thanks to the wearable holographic nano-layer catalyser".* The device appears identical to a £5 USB key, with the addition of a sticker.

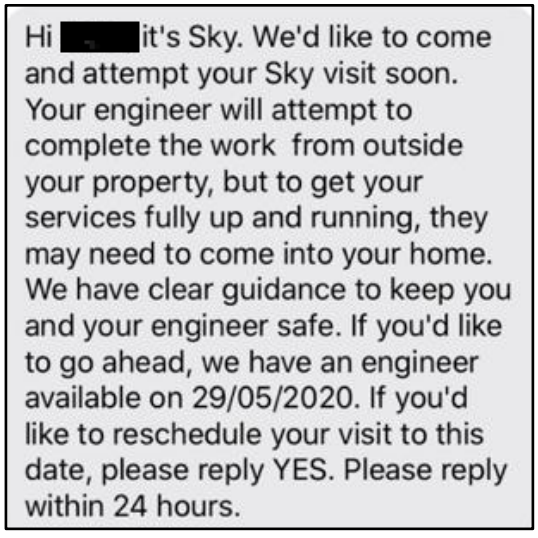
## Scams

Scam texts purporting to be from Sky, GOVUK and HMRC are being seen and reported locally, with examples given below:

*"I received notification of the Sky engineers visit earlier in the week scheduled for 1 June and a text message from the Sky messaging service on Sunday as a reminder and the engineer called yesterday. I have changed my sky password, blocked this number and deleted the message."*

*"Just had a call from 01227 126302, a recorded message from HMRC stating there was a tax fraud against my name. I didn't get to the end of the message deleted and blocked the number."*

*"GOVUK: You may be eligible for a COVID-19 relief fund of up to Â£1,500.00 please complete the application form with the link below to check your eligibility."*




The link appears to be a gov.uk form on google docs. First page asks for name and address.

East Midlands Special Operations Unit

## Hot topics

CIFAS warn of a new HMRC scam, specifically targeting people who are out of work or working less due to coronavirus. The scam claims to offer thousands in grants and recipients are told to click a link to check eligibility. The questions asked on this link are designed to steal personal information. The email address used in this scam is: HMRC@hotmail.com.

**Courier Fraud:** Criminals impersonating bank officials and police officers, is still a hot topic.

**Key advice:** Can you always trust who is on the end of the line?

- When in conversation with someone you don't know, before answering a question make sure they need to know the information that they're asking about.
- Don't get caught up in the story being told; a sense of pressure should be a red flag.
- Hang up, wait five minutes, make sure you can hear a dial tone before making any other calls, or use your mobile.

Verify any unexpected contact is genuine by using a known number or email address to contact organisations directly (101 for Police; Tel number on your Bank card).

To register for the free ActionFraud email or text alert service click 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.

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

**Webinar – Monday 8th June 2020 @ 1400 – 1500 hrs**

### Ransomware - Hostage taking your data

**The MPS Cyber Crime Unit discuss Ransomware, what it is, what it can do, and what you need to do to protect yourself and your company.**

### About this Event

Ransomware is a persistent threat in the world of cyber security. In this webinar members of the Metropolitan Police Cyber Crime Unit, along with a member of the National Cyber Security Centre will discuss this malware. A representative from a company, Air Marine Ltd, who were victim of a ransomware attack in 2019, will also be participating, explaining his experience of this crime.

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