East Midlands Special Operations Unit

# COVID-19 CYBER AND FRAUD PROTECT MESSAGES

*Wednesday 29 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.**

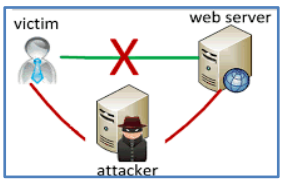
**Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.**

**If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team or your local Force protect team.**

## Today's cyber topic is 'Man in the Middle and Whaling'

As we continue to see criminals rehashing previous schemes with Covid19, its worth remembering that some techniques are centuries old. The Spy master Sir Francis Walsingham employed these techniques to intercept and decode messages between Mary Queen of Scots and her sympathisers, whilst held captive by Elizabeth I.

Walsingham, reporting to Elizabeth, created an easy way for Mary's agents to smuggle messages in and out, whilst unknown to them he intercepted them. He then relayed the messages on to Mary's supporters, using the information gained to defeat Mary's plans to overthrow the monarchy, an early **"man in the middle"** attack.




The modern **"man in the middle"** may be setting up fake Wi-Fi hotspots, in public areas, to catch the unwary as they log on. Copying the data as it is passed on to a genuine Wi-Fi hotspot. Be wary of free Wi-Fi, if accessing sensitive data, using 4G is more secure.

Walsingham also used his knowledge of Mary to send out messages, supposedly from her, to trick her supporters into divulging their plans and name other sympathisers.

Modern criminals also use knowledge, gained from the digital footprint of their target, in **Whaling;** a highly targeted phishing attack aimed at senior executives and masquerading as a legitimate email. Whaling is designed to encourage victims to perform a secondary action, such as initiating a transfer of funds. Whaling doesn't require extensive technical knowledge yet can deliver huge returns. As such, it is one of the biggest risks facing businesses.

The adoption of fluent business terminology, industry knowledge, personal references and spoofed email addresses have made sophisticated whaling emails difficult for even a cautious eye to identify. Highly targeted content is now combined to either exploit existing trusted relationships, or combine a cyber-attack with fraud tactics.

### Whaling email with a phone call

This is a social engineering tactic which could be described as cyber *enabled* fraud. The phone call corroborating the email request, making the victim complacent about a possible cyber-attack, as they have also had a 'real world' interaction.

East Midlands Special Operations Unit

With the growth in remote working criminals are exploiting the lack of easy access to decision makers which hinders the querying of requests.

**Making your employees aware of social engineering threats doesn't make them invulnerable; some attacks are too well crafted and no amount of user awareness and training can guarantee their detection**. Training on social engineering tactics should be part of a defence against attacks, but recognise the limitations of such measures.

Organisations should accept that a successful whaling attack is a possibility, and put in place checks and processes to mitigate the damage. Make sure all staff are aware of them and encourage staff to question any urgent or unusual demand – Criminals will try to put staff under pressure and staff should be encouraged to query unusual transactions.

More detailed advice and guidance from the NCSC can be found here

## Hot topics

- A Covid19 phishing email scam began by infiltrating a firms' email accounts and observing email activity to understand the different channels used to conduct money transfers. Any interesting emails were diverted into a folder monitored by the criminals, who then registered lookalike domains. Emails were sent from these lookalike domains and once the attackers learned how money transfers were executed, they used the lookalike domains to instruct new money transfers.
- Phishing emails purporting to be from on line betting companies, offering customers free bets are appearing. If it sounds too good to be true, it probably is. Never click on links in suspicious emails.
- Phishing emails purporting to be from the WHO continue to be sent out, with request for donations or suspect links.
- Amazon Gift Cards have been requested in some reports over the past week.

**Webinar - Thursday 30th April 2020 @ 1400 – 1500 hrs**

This week's topic: **Online fraud…Evolution or Repetition?**

City of London Police's Cyber Griffin team take a closer look at online fraud. The panel of experts will be taking your questions and answering the following:

- Why is online fraud so prevalent?
- Are criminals using new and unique methods, or just repackaging age old techniques?
- How can people and organisations avoid becoming victims?
- What does the future of online fraud look like?

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.