Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Thursday 16th April 2020

Today's topic is a review of some of the most common themes, hot topics and trending news of the last few weeks.

Fake News continues to be a problem

Mainstream media (BBC/ITV) report the spread of false information during the coronavirus outbreak has been rapid. People sharing messages on social media warning of everything from beating the virus by drinking hot drinks to 5G masts spreading the virus.

There has also been a lot of 'noise' in the press and social media about scams and advice is being offered from all sources.

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

Current Fake News example:

A WhatsApp audio message that is being forwarded on social media stating "facts" about coronavirus. It is made to look like it's been leaked by someone working with the ambulance service, states that on Thursday (9 April) the UK will hit its peak and face 900 deaths per day from coronavirus. The hoax states that one third of the 900 deaths will be babies, children and teenagers with no underlying health issues and goes on to suggest that people will be told to manage their symptoms at home and no ambulances will be sent to patients, even those who are struggling to breathe.

"This is fake news, and we would urge people to ignore the message and not share it further". – ***Professor Viv Bennett, Chief Nurse at Public Health England***

Hot Topics

Action Fraud warn the public about the continued use of the NHS in scam messages requesting either money or personal details.

Text messages are being sent to dupe people into topping up their mobile phones as they cannot visit shops.

A Covid-19 scam via text and WhatsApp telling people to claim a supermarket voucher, is now also appearing as an email. The victim clicks the link and enters personal info.
Coronavirus-themed phishing attempts continue. People are being duped into opening attachments, which then compromise their personal information, email logins, passwords and banking details.

Fake medical products and testing kits for COVID-19 continue to be offered online.

HMRC phishing email scam in which individuals are asked to complete a "coronavirus relief form" in order to receive payment within 2 days.

HMRC demand for payments of corporation tax using a photo shopped letter

Who is listening in to your conference/work calls - Alexa, Siri or Google Assistant?
These devices are **ALWAYS** listening - be mindful of your location.

Having a confidential or sensitive conversation?
Move to another room or turn off the smart speaker

Trending

Hackers are sending a new COVID 19 email titled "You are infected". Recipients are asked to download an infected Excel document attached to the email and proceed to the nearest emergency health clinic for testing.

Phishing emails purporting to come from Microsoft or internet browsing companies asking to click on link for terms and conditions update.

The National Pensioners Convention has received reports of COVID-19 scams specifically targeting the elderly, such as selling pre-paid funerals and power of attorneys.

Scam email, stating the following: *'As schools will be closing, if you're entitled to free school meals, please send your bank details and we'll make sure you're supported'.*

ZOOM video security - There are several reports in the media, raising doubts about the security of ZOOM. We recommend that users review the set up and implement all of the recommended security setting within the application.

Top tips for video users:
Think about location - what can be seen in the background?
Do you have Alexa, Siri or Google Assistant listening in the background?
Sharing your screen – think about what else can be seen when you "share"

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution 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 ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.