East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Tuesday 14 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.

Following the Easter break we have reviewed the recent reports issued by Action Fraud, NCSC etc and summarised the most common themes, topics and trending items.

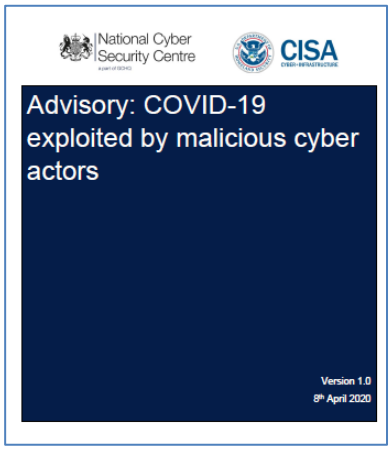
Hot topics

UK domain name registrar Nominet has taken down over 600 coronavirus scam sites. These websites have been selling fake vaccines, protective equipment and frauds remedies related to coronavirus. The company is filtering all coronavirus-related content in a bid to stop scams and disinformation from being spread. (Source – ZDNet)

Analysis of recent COVID-19 cyber activity found that 65% of coronavirus phishing campaigns were delivering spyware, 31% delivered backdoors and 4% delivered ransomware.

AgentTesla and NetWire collectively made up 75% of delivered malware. Other malware included LokiBot, HawkEye, Aurora, Hekbit, Formbook, and other unclassified spyware.

US-CERT, CISA, and the UK NCSC have issued a joint security advisory surrounding an increase in COVID-19 related themes by malicious actors for SMiShing, phishing for credential theft, and phishing for malware deployment. The full security advisory from the NCSC can be found **here.**



A new COVID-19 themed phishing campaign is distributing the HawkEye malware in RTF documents. This campaign has targeted multiple organisations in the healthcare sector, and claims to provide information for treating the virus or curing it altogether. Full technical analysis can be found **here** at the source.

East Midlands Special Operations Unit

Coronavirus-themed phishing attempts continue. People are being duped into opening attachments, which then compromise their personal information, email logins, passwords and banking details.

Trending

COVID-19 themed emails pushing the infamous AgentTesla infostealer. The emails mention a “Stimulus Package”, imitating the compensation plans that the UK, and others are offering.

Microsoft claims that there has not been a sudden surge in malicious attacks in light of the pandemic, but rather an influx of ’re-themed' attacks. Attackers have not gained more resources, but are instead repurposing their existing phishing, ransomware, and malware infrastructure to include COVID-19-themed keywords in a bid to infect more users.

Reports have been received of scammers calling to sell coronavirus insurance.

Reports also received of website offering COVID-19 antibody blood tests.

Microsoft are reporting covid-19 related cyber-attacks in 241 different countries and territories. Every country in the world has seen at least one COVID-19 themed attack.

Phishing emails purporting to be from PayPal are being sent out with the subject line indicating s that this is COVID-19 related. The email states that due to new updates, the users account has been limited and provides a link for the user to fill in their details.

Social media campaign

With so many young people with time on their hands the NCSC and NCA will be promoting a series of posts encouraging those with an interest in tech to make use of more time at home to start the discussion about how to put their skills to good use, to make sure they're staying safe online and use their free time to improve their skills and stay safe online.

Reporting

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