CYBER AWARE

south east
Regional Organised Crime Unit

Cyber-crime & Coronavirus

Newsletter – April 2020

Coronavirus SCAM ALERT

National Cyber Security Centre
a part of GCHQ

Coronavirus, or COVID-19, is having a huge impact on our communities. Self-isolation, social distancing and concerns over relatives has led to a huge increase in anxiety and apprehension. Regrettably, such circumstances are seized upon by cyber criminals and the current pandemic is no exception. There has been a huge increase in cyber-attacks since the start of the pandemic with cyber-criminals preying on the fear and uncertainty of both individuals and businesses alike. This month's newsletter seeks to raise awareness across all our communities – both individuals and businesses to minimise the risk presented by this increased criminal activity.

What kind of attacks are taking place?

Phishing e-mails are abundant. Internet security companies have numerous examples on their websites but as with all phishing e-mails, scammers will post claims that may offer treatment or cures for COVID-19. These will inevitably convey a message of urgency — for instance, 'Buy now, limited supply.' Plenty will look very real as the scammers are using logos and domain names that look identical to the organisations providing legitimate information. In addition, many of these phishing emails will contain links and attachments that purport to contain updates and information about the situation. Clicking these links or opening the attachments may well infect your device.

In addition to a huge increase in phishing e-mails, bogus charity collectors are hard at work 'collecting' on behalf of charities that are non-existent. Scammers are asking for crypt-currency donations for help in researching a cure for the virus. Others may try selling medical equipment, medicines or masks that will never arrive after payment is taken. Phone scammers are calling randomly to try and trick us into accepting remote connections or other services based on the COVID-19 uncertainty.

There has been a significant increase in cyber-attacks directed at businesses with the delivery of ransomware increasing considerably. These attacks are designed to take place at a time where businesses are extremely vulnerable

Useful Links

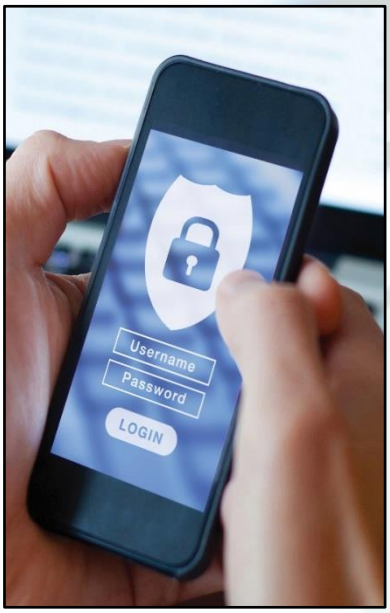
SEROCU: www.serocu.police.uk/organisations
NCSC: www.ncsc.gov.uk

CYBER AWARE

south east
Regional Organised Crime Unit

and extra care needs to be taken when interacting with e-mails and undertaking online activities. Many workers are now working from home in accordance with Government advice and face several different cyber challenges – not least the requirement for connecting to networks through some form of remote desktop protocol.

What do I need to know?



The NCSC is urging businesses and the public to consult its online guidance, including how to spot and deal with suspicious emails as well as mitigate and defend against malware and ransomware. If you do receive phishing e-mails relating to the COVID-19 pandemic, please forward them to the Action Fraud portal: -

https://www.actionfraud.police.uk/report-phishing

For any online activities, including connecting to your business network, make sure you are using a strong password formed of three random words, obfuscated with letters and symbols – as discussed in our February newsletter. Wherever possible, please setup and use 2-factor-authentication. Individuals and businesses are encouraged to create an offline backup of their critical data at regular intervals to mitigate against the risk of ransomware attacks. Whilst backups should be considered a last option, they are critical to getting your business back up and running in the event of an attack. Keep your devices, software and apps up to date and ensure you have current anti-virus software on all of your devices.

And finally, if you want more information about COVID-19, use legitimate resources. Most news channels are broadcasting information 24 hours a day and for those with medical or financial concerns, consider using genuine government or NHS websites.

What else is happening to protect me?

In recent days, the NCSC has taken measures to automatically discover and remove malicious sites which serve phishing and malware. These sites use COVID-19 and Coronavirus as a lure to make victims 'click the link'. Countries across the world are working together to minimise disruption caused by these criminals. It is vital that we all contribute to these efforts – reporting cyber-attacks and phishing where possible and following NCSC advice.

Where can I find more information?

Suspicious E-mail: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Remote Working: https://www.ncsc.gov.uk/guidance/home-working

Advice & Guidance: https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Government Advice: https://www.gov.uk/coronavirus

NHS Advice: https://www.nhs.uk/conditions/coronavirus-covid-19

Useful Links

SEROCU: www.serocu.police.uk/organisations

NCSC: www.ncsc.gov.uk