In the know
Surrey and Sussex

Sussex

Covid-19 Scam Alert

25th March, 2020

Coronavirus (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, these circumstances are seized upon by criminals both on and offline. There has been a huge increase in cyber-attacks since the start of the pandemic with cybercriminals preying on both individuals and businesses alike, as well as criminals posing as samaritans wanting to help their local community.

What kind of attacks are taking place?

Online

- **Phishing e-mails**: Scammers claim to offer treatment or cures for COVID-19 such as medical equipment and supplies. These will likely convey a message of urgency such as, “Buy now, limited supply!” These items will never arrive after payment has been taken from you. They can look very real as the scammers are using logos and domain names that look identical to the legitimate organisations. They may also contain links/attachments to updates and news on the pandemic which can harm your device if clicked on.
- **Fundraisers**: Bogus charity collectors ‘collect’ on behalf of charities that are non-existent. Scammers are asking for crypt-currency donations for help in researching a cure for the virus.
- **Businesses**: 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 and extra care needs to be taken when interacting with e-mails and undertaking online activities.
- **Working from home**: 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. Ensure the process to connecting to work systems is detailed by your employer and followed with care.

Offline

- **Doorstep Callers**: Remain vigilant when having doorstep visitors, particularly if it is someone unfamiliar. Our community has found new and supportive ways to get together and help others, however, some people are choosing to use this as a cover to profit from exploiting our anxiety and concern.

What can I do?

Online

The National Cyber Security Centre (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

- **Online activities**: Make sure you are using a strong password formed of three random words, mixing letters and symbols.
- **Back up**: Create an offline backup of critical data at regular intervals to reduce the risk of ransomware attacks. These are critical to getting your business back up and running in the event of an attack.
- **Update**: Keep your devices, software and apps up to date and ensure you have current anti-virus software on all of your devices.

Offline

- **Doorstep Callers**: Criminals may call at your house posing as officials or offering you help whilst in isolation/lockdown.

Take 5 steps to reduce your risk of becoming a victim:

1. **If you're not sure who is at your door, don't open it**. If you have a door chain put it on before opening the door or speak to the caller through a closed door.
2. **Check the identity of the caller**. A genuine caller will happily wait outside while you check their identity and by calling their organisation they are claim to be from. Don't use any telephone numbers provided by the caller as they may be bogus.
3. **Call a neighbour or friend to assist**. If you are still concerned, telephone a neighbour or friend nearby to come along and check out the caller before you open the door to them
4. **Caution**. Never let anyone in your house unless they are someone you know and trust. It's ok to say No and tell them to leave.
5. **Keep doors locked and windows secure at all times**. Stop anyone from entering your house through open or insecure doors and windows.

Report. If you suspect a bogus caller has visited you, even if you didn't let them in, call Sussex Police straight away on 101 or on 999 if you believe a crime to be taking place.

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
Sussex Police Crime Advice on Fraud & Scams: https://www.sussex.police.uk/advice/advice-and-information/fa/fraud/

Kind Regards,
Brighton & Hove Prevention Support Team

Message Sent By
Sarah Donaldson-Alldis (Police, Prevention Support & Engagement Officer, Sussex)