DIIU Cyber Update

Coronavirus Cyber Attacks

Advice and guidance for businesses during the Covid-19 Pandemic

We are already seeing, on a national level, increasing and targeted threats against a variety of targets. We have seen previously the impact a cyber-attack can have with the Wannacry Ransomware attack in 2017 on the NHS. An attack could have a more damaging impact in this period as businesses themselves, their IT companies and wider cyber security industry have less capacity to respond quickly to mitigate the damage with high levels of staff abstracted through sickness and self-isolation. Below we have some advice and guidance on some of the biggest threats at this time and what you can do to protect your business.

Ransomware

Ransomware is a form of malware that, when it gets onto your computer, will encrypt all your files making them unreadable. Ransomware can spread throughout a network, meaning the potential impact on a business can be huge.

The best thing you can do to protect your business is to keep a regular up to date backups of all your business critical files. By doing this you can recover your data without having to pay a ransom.

For lots more on protecting your business from Ransomware then see the guidance from the National Cyber Security Centre here - https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Home Working

Following government advice, many businesses and organisation that can, have instructed employees to work from home. While this won't be new to many, you may have an increased number of employees working from home than normal and for a longer period of time. More advice about preparing your business and staff for home working here - https://www.ncsc.gov.uk/guidance/home-working

Our top tips for employees working from home:

- Change default passwords on home Wi-Fi router
- Use different and strong passwords on every account and device
- Keep all devices, apps and operating systems up to date
- No one else has access to your device e.g. children
- Working in a more public place? Then watch out for shoulder surfing

Phishing - a major threat

No topic is ever safe from phishing and Covid-19 is no exception. Cyber criminals are exploiting this online by sending phishing emails claiming to have important updates, information on cures, encouraging donations and even impersonating the World Health Organisation (WHO).

It's really important to make staff aware of the types of phishing emails being seen that is linked to the Covid-19 pandemic but also a time that can be used to remind staff how to spot and deal with phishing emails. Guidance can be found here - https://www.ncsc.gov.uk/guidance/suspicious-email-actions

We update regularly on our social platforms which you can follow.
Twitter - @WP_CyberProtect (https://twitter.com/WP_CyberProtect)
LinkedIn – Kieran Hall (https://www.linkedin.com/in/kieranhallqi/)

For any questions regarding the above feel free to email us.
Lee.stripe@wiltshire.pnn.police.uk or Kieran.hall@witlshire.pnn.police.uk