Wiltshire Police

Business Cyber Update

April 2020

The way we work has changed, at least for the time being. Covid19 has seen our daily lives restricted in an unprecedented way and that has bought with it some challenges for the workplace. Your business may already be used to remote working, or you may be doing it for the first time, but one thing is certain…. There has been a huge rise in home working.

With the increase of home working has come the rise of cyber criminality. Latest figures from Action Fraud, the national reporting centre for fraud and cyber crime, already show a loss of over £2 million just for covid19 related reports, and with cyber crime known for being under reported we suspect there's more.

Why is home working a threat? Working from home won't be new to many businesses and their employees, however covid19 is forcing you to consider home working on a much larger scale, and for an extended period of time. You may have some employees who haven't done it before and will need to set up new accounts, it's vital your new users set up with strong passwords.

You may also require new services or to adapt current ones, so that teams can work together. In the rush to get everyone up and running security may have not been at the front of your mind. Now is the time to go back and check. Is it up to date, being regularly patched and users given correct level of access?

Virtual Private Networks (VPNs) permit remote users to securely access your businesses IT resources, things like email and file servers. It's an encrypted connection over the internet from a device to a network, ensuring that sensitive data is safely transmitted and prevents unauthorised people from accessing your data. Make sure you're VPN is fully patched. Extra licenses or bandwidth may be needed or if you've not used one before the NCSC's VPN Guidance can help you get started.
One other thing to quickly note is looking after devices. Staff are more likely to have devices stolen or lose them when outside of the office environment. Encourage staff to lock screens if left unattended, when not in use store it somewhere safe, and who to report to for any losses. Ensure staff keep devices up to date and that they know how to do this.

Cyber criminals are opportunistic and will look to exploit any event, it's no surprise that they're exploiting the coronavirus online. The most common method used is phishing, when criminals try to convince you to click on links within a scam email or text message, or give sensitive information away.

We've seen ones that claim to have a 'cure' for the virus, offer you a financial reward or encourage you to donate. These aren't new methods, they are existing ones, just reconfigured to use the pandemic as a hook and are designed to get you to react without thinking it through fully. Businesses looking at buying protective equipment have been targeted with phishing emails linked to fraudulent domains selling non-existent goods. Another method being used is emails with malicious attachments. Likely containing ransomware, the emails are either impersonating high level individuals within the business or other organisations. Once opened these can encrypt all your files and try to spread to other machines on the network. The vital action to take to mitigate ransomware is to ensure that you have up to date backups of important files. If so, you will be able to recover data without paying a ransom. Having a security solution installed could prevent it from running if opened and keeping devices and software up to date will keep you protected against the latest threats.

Proactive work is being done to target phishing and the takedown of domains supporting it. The Nation Cyber Security Centre (NCSC) have been taking down domains linked to exploiting covid19 and on 21st April launched a new Suspicious Email Reporting Tool. Forward the email to report@phishing.gov.uk, if the email contains links to malicious sites, the NCSC will take down or block those sites.

Spotting a phishing email can be hard, they are becoming more believable and even that savviest people can be tricked. There are some common signs to look out for:

- Authority – usually claiming to be someone official
- Urgency – given a limited time to respond to the request
- Emotion – praying on fears, curiosity or hope
- Scarcity – offering product in high demand

If the message was unsolicited, unexpected or from a regular contact but unusual then be cautious, don't click on any links and check the authenticity of the message with the person or company first before acting.

More advice and guidance can be found on the NCSC's website, our social pages on twitter - @WP_CyberProtect, and Facebook - Wiltshire Police Cyber. And, when we're allowed out again we hope to see you at future events.

Lee Stripe & Kieran Hall
Cyber Protect & Prevent Officer
Digital Investigations & Intelligence Unit
Wiltshire Police.