Working From Home

Top tips to protect your staff and business against cyber crime

The rapid spread of coronavirus left many businesses with very little time to adapt to a new working life from home. With such a significant transition to make, businesses without prior experience of operating an agile workforce had to adjust with limited preparation. Taking advantage of this rise in remote working, The National Cyber Security Centre (NCSC) has revealed that criminals are exploiting the public's fears around coronavirus and are persistently targeting victims through various forms of media. In terms of business, under the General Data Protection Regulation (GDPR), failure to protect customer data is punishable by fines of up to 4% of your company's turnover in the previous financial year. It is therefore vital that adequate security protection mechanisms are installed, up-to-date and fully active on all functioning devices to reduce the risk of data breaches. This article will therefore deliver some top tips to help protect you and your staff from cyber crime during this time of global online vulnerability.

Use virtual private networks (VPN)

Ensure that all your remote staff are connecting their devices to a secure VPN. In doing this, private data is transported across unknown networks, including home routers and this can prevent the exposure of passwords and IP addresses. It's important to make sure that the VPN is fully patched and has sufficient licenses for the entire workforce. In addition, depending on business requirements, it might be valuable to consider blocking traffic to traffic consuming websites, such as social platforms, in order to manage the burden of the network.

Implement cloud security

Cloud services and containers are also prime targets for attackers, so for those who work in these environments, a cloud security solution should be implemented in order to check for vulnerabilities. Such solutions not only enable a safe migration to this environment if you are new to working in this space, but will also continuously monitor for misconfigurations and compliance issues.

Install firewalls

Firewalls should be installed to protect your staff's individual work devices, personal devices (if these are being used for business) as well your entire computer network from unauthorised external access attempts. Personal firewalls are installed onto the devices that require protection and monitor the data traffic that flows between the device and the network it uses. Alternatively, external firewalls offer a more robust security defence mechanism. Although more expensive than personal firewalls, the external option means that the protective software does not operate from the system it is protecting, therefore making interference and manipulation much more difficult. If your staff are connecting from home networks, smaller Single Office/Home Office (SOHO) firewalls can also be installed for their homes. These operate behind the users' own firewalls and can isolate them from the rest of their home network.

Ensure that devices are encrypted

Making sure all company devices are encrypted is another essential way to limit cyber crime. Data protection features such as Bitlocker offer full volume encryption which protects data if devices were to be lost or stolen. Such features therefore help mitigate the risk of unauthorised data access, protecting you and your business from facing the potential consequences under GDPR. Running outdated software and apps also increases the opportunities for cyber criminals to operate. Particularly with sensitive data, it is important to ensure that your staff are updating their devices regularly so that weaknesses are limited.

Understand the threat that ‘phishing’ poses and minimise your risk of becoming a victim

The NCSC has recorded a drastic increase in ‘phishing’ attempts since the onset of coronavirus, threatening both the general public and businesses. Fake emails claiming to contain important information encourage victims to click on links, which then infect the device and can lead to loss of both money and sensitive data. Ensure that your staff are aware of the threat and have seen examples of how these attempts are usually presented so that they can remain vigilant whilst working remotely. To limit the risk, you can effectively reduce your attack surface by having a full, professional security assessment which can identify and prioritise your current vulnerabilities. By ensuring the installation of up-to-date antivirus software, if a link were to be clicked, running a full scan using this software will help to clear up any initial problems. Web filtering software is also a useful protective measure against phishing. It filters out malicious websites so that if the user does click on a link and they unknowingly try to access a dangerous domain, the software will block the request and take them to a block page.

Uphold your brand’s reputation through the implementation of anti-spoofing measures

By implementing anti-spoofing measures on your domains, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC), you can make it difficult for fake emails to be sent from your organisation. Using Transport Layer Security (TLS), you can also protect your business’ emails in transit. This should not be overlooked, even if your organisation uses popular Cloud email providers, such as Google G Suite and Microsoft Office 365.

Encourage multi-factor authentication (MFA)

Encourage your employees to scale up MFA on email, social and banking and emphasise this particularly to those with access to networks and critical applications. Doing this reduces the risk of being hacked as they will be asked to provide two or more pieces of evidence before they are granted access. It’s actions such as this that can have great significance if your business were ever to be a target of cyber crime.

If you’d like to find out more about how to get started, please get in touch.