Remote working guide
Coronavirus (COVID-19)

As part of efforts to manage the spread of coronavirus (COVID-19), many organisations have mandated or are encouraging their employees to work from home. This is almost certainly the first time ever that such a huge percentage of the working population will be working remotely at the same time.

While this is an indicator of the progress we have made, we must also highlight the potential security challenges businesses will face. Many applications, which support remote working, have already reported additional stress on their resources, with some experiencing periodic outages. For many individuals, this may be their first time working remotely, or at least they are less familiar with the concept.

It is no surprise that cyber criminals prey on victims in their most vulnerable moments. In this current climate, threat actors will be inclined to take advantage of the situation. Some of the top threat's businesses may face with their employees working remotely include:

1. phishing – in the last couple of weeks, there has been an influx of coronavirus-themed phishing emails. Cyber criminals have taken advantage of the current anxiety and thirst for information by sending out phishing emails with information on COVID-19 such as vaccines, tax refunds, preventive measures from the 'World Health Organisation' etc. Clicking on links or attachments contained within such emails takes victims to a fraudulent page that harvests their information, including login credentials and financial and tax information. An F-Secure blog post lists typical coronavirus-related phishing email titles.

2. VPNs – remote working, in most cases involves the use of a virtual private network (VPN). Only a few months ago, several VPN appliances were found to have critical vulnerabilities – for which patches have been released. VPN devices need to be internet facing, which makes it easy for attackers to scan the internet for these vulnerabilities. These vulnerabilities give attackers remote access to a network without login credentials.

3. stretched IT staff – similar to holiday periods, many organisations are dealing with fewer available IT staff (and possibly more distractions). This will most likely cause problems in terms of operations as the few available staff may be overworked, unable to detect issues or manage resources etc. In addition, in this time of enabling remote working for as many staff as possible, support teams are more inclined to be ease-of-use focused rather than security-focused, meaning their guard may be down to some extent.

What can businesses do to protect themselves?

- We urge businesses to alert their employees on potential incoming phishing emails. Employees should be trained to spot and manage phishing emails. Hiscox currently offers the Hiscox CyberClear Academy, a free cyber awareness training platform, to all of its cyber insurance customers. The platform also contains helpful modules such as '**bring your own device (BYOD)**' and '**remote and mobile working**'.
- Enable multi-factor authentication (MFA) on user accounts, especially administrator accounts.
- All VPN hardware and software should be patched and up-to-date.
- Anti-malware software, IDS/IPS (intrusion detection/prevention software) etc. should be up-to-date.
- Close all unnecessary open ports.
- Use only applications recommended/vetted by the business.
- As far as possible prevent users connecting personal devices to corporate networks unless they are segmented or operate in a 'sandboxed' environment to prevent cross-contamination.

Several authorities have published guidance on remote working such as the UK's NCSC and SANS institute.

Hiscox
1 Great St Helen's
London EC3A 6HX
United Kingdom

T +44 (0)20 7448 6000
E enquiry@hiscox.com
www.hiscox.co.uk

20606 03/20