datacentrix

eCentrix – April 2020

11 essential steps to reinforce cybersecurity in the age of COVID-19

The sudden, radical move to remote working during this time of lockdown for South Africa brings with it the promise of a new and more effective way of working – without being bound to a physical office. Not only does this surge in the use of remote work capabilities have massive implications on the corporate culture and on productivity levels; but it also brings with it more immediate consequences from a security and privacy perspective that cannot be ignored.

So says Wayne Olsen, head of the security business unit at Datacentrix. Together with the team of security experts at Datacentrix, Olsen has compiled a guideline of ten steps to ensure that businesses and their employees are protected while working remotely.

1. Use only devices approved by your organisation.
"It is critical that staff avoid using personal computers and tablets – as well as those shared with others – to work. Other users may have inadvertently performed activities that infect shared devices, or cause leaked information," Olsen explains.

2. Use the virtual private network (VPN) when necessary.
"VPNs, which provide secure direct connections to an organisation's network, might be necessary when accessing files, working with sensitive information, or using certain websites. At home, workers should remember to update their router's software and secure it with a lengthy, unique password."

3. Think before you click.
Olsen advises remote workers to avoid downloading or clicking on unknown links in emails – always verify the identity of the sender, double check the authenticity and accuracy of the sender's email address and verify the request with your employer if you are uncertain.

4. Beware of coronavirus-themed phishing e-mails.
"Cybercriminals are exploiting the coronavirus outbreak by sending fake emails, including dangerous links, to employees," he states. "Here's how it works. The email messages may appear to come from company officials and might ask you to open a link to a new company policy related to the coronavirus, or to enable remote access to the company's VPN. However, clicking on the attachment or imbedded link will most likely download malware onto your device. Don't click. Instead, immediately report the phishing attempt to your employer."

> "Just as everyone is responsible for helping to prevent the spread of the coronavirus by changing their behaviour; everyone is also accountable – as cyber citizens – to ensure that we protect ourselves and our companies from the ever-growing security risks posed by COVID-19.

5. Guard your devices.
If your organisation allows you to work from your home, never leave your laptop, tablet or mobile phone (including any USB or external storage devices) unattended, warns Olsen. "Another point that should be top-of-mind is to avoid entering passwords where others can see them."

6. Create strong passwords.
“These must include a mix of upper and lowercase letters, numbers and symbols. Make them difficult enough that someone can't guess them.”

7. Don't share passwords online.
If you must share log-in information with a co-worker, says Olsen, call them with the details instead of sending via email, text or instant message.

8. Use two-factor authentication.
“Although it can be inconvenient, two-factor authentication, if available, provides an extra layer of security to keep hackers from accessing accounts.”

9. Update your devices.
“If you are using a personal device that has been approved for teleworking, be sure that it is running the most current operating system and that your web browsers and other applications are also up to date,” he adds. “Also, confirm that you are running the latest antivirus software solution. Updates include important changes that improve the performance and security of your devices.”

10. When in doubt, contact your organisation, or your ICT service provider's helpdesk.
“Remove the guesswork by allowing the professionals to advise on actions that are in line with your business' cybersecurity practices and procedures. This way, you can ensure that you aren't opening up your devices – or your corporate network – to cyberattacks.”

11. Don't forget about securing video conferencing solutions.
“Video conferencing solutions have been a boon for companies across the globe, allowing them to continue to run internal and external meetings but on a virtual level. However, some platforms have come under scrutiny from a cybersecurity perspective, with individuals joining meetings as uninvited guests and claims of users' social media pages being hacked.

Whatever the video conferencing solution being used, businesses need to check that employees are aware of potential vulnerabilities and take steps to tighten security measures on these platforms.”

Wayne Olsen, head of security business unit at Datacentrix

“Just as everyone is responsible for helping to prevent the spread of the coronavirus by changing their behaviour; everyone is also accountable – as cyber citizens – to ensure that we protect ourselves and our companies from the ever-growing security risks posed by COVID-19. Hackers do not discriminate and are making use of this pandemic for financial gain. It is important that we all remain cautious and follow the guidelines in order to mitigate all of these risks,” he concludes.