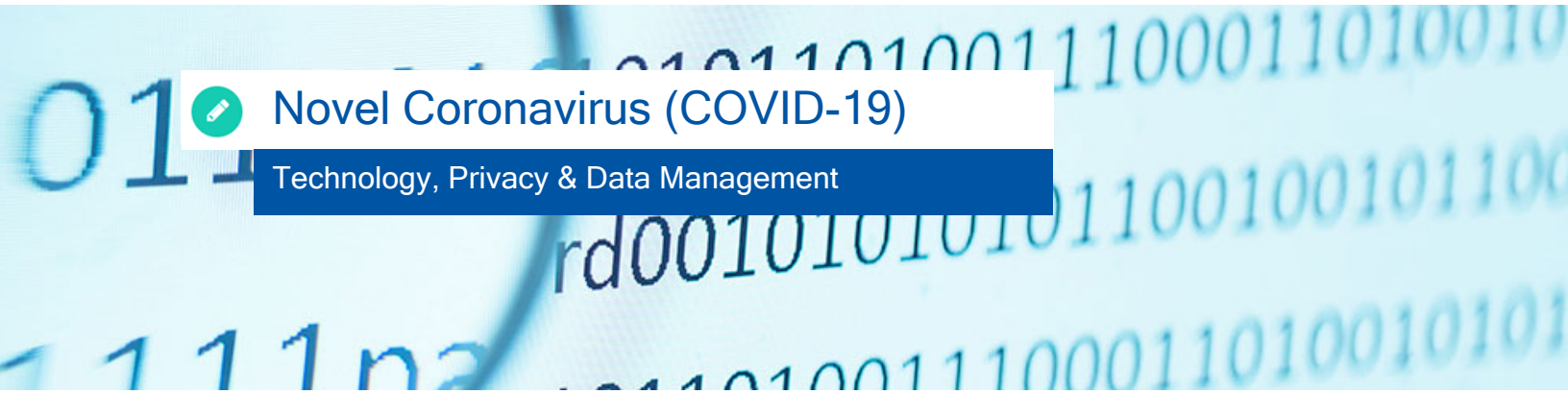
Torkin Manes
Barristers & Solicitors



Novel Coronavirus (COVID-19)

Technology, Privacy & Data Management

April 2020

Cybersecurity in the time of pandemic

Safe computing still needs to be practised while working from home

By Lisa R. Lifshitz

As we hunker down in our home offices and try to protect ourselves from the ravages of COVID-19, it is worth remembering that, in addition to the threats posed by the virus, we are also increasingly at risk from scammers and hackers seeking to exploit existing cybersecurity gaps (and our general sense of panic) through various phishing and spear-fishing campaigns and malware scams.

Preying on users' cybersecurity weaknesses is not new. What's different now is that many employees are novice remote workers who may not have had the time or ability to fully protect their at-home work environment. In our haste to obey mandatory municipal, provincial, territorial and federal self-isolation and stay-at-home requirements, some companies have scrambled to provide their workers with adequate and necessary hardware, and may not have fully considered and protected against security threats, i.e., ensuring critical systems and corporate software have been fully updated and patched, or provided employees with supplementary security training.

In some instances, the need for speed – to ensure business continuity and continue to serve clients – has resulted in poor cyber-hygiene, even as workers scramble to make do with a combination of work-provided and unvetted personal devices and vulnerable Wi-Fi networks. Employees who are trying to show their companies that they are still labouring diligently can easily be misled by hackers pretending to be their boss, or by co-workers sending them authentic-looking emails asking them to provide critical network credentials or other confidential/private information.

Phishing – defined by the Canadian Centre for Cybersecurity (CCC) as attempts by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific and usually a well-known brand, normally for financial gain – typically involves attempts to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Spear phishing involves the use of spoofed emails to persuade people within an organization to reveal

their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scale and well-targeted.

Hackers also use email to deliver malware, malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware and adware.

To date, there have been myriad examples of scammers trying to trick the unsuspecting public through the use of phishing, spear phishing and malware. As reported by the CBC on March 30, virtual private network provider Atlas VPN has determined that the number of active websites used for phishing has increased by 350 per cent between January and March, just as the COVID-19 crisis erupted. Barracuda Networks, based in California, has reported a 667 per cent spike in phishing emails from the end of February until late March.

Canada's Communications Security Establishment (CSE), the parent agency of the CCC, has been kept busy identifying and taking down malicious websites spoofing Government of Canada websites (e.g., the Public Health Agency of Canada and the Canada Revenue Agency) that were spreading COVID-19 misinformation, and the CSE has also reported cases of maps showing the outbreak of COVID-19that infected devices with malware, phishing emails with malicious links and attachments, and spoofed COVID-19 websites. The CSE's March 23rd alert noted several examples of these COVID-19 phishing attempts, with such tantalizing email subject lines as:

- Cancel shipment due to corona virus _ New shipping schedule details
- Corona is spinning out of control
- Feeling helpless against Corona?
- Military source exposes shocking TRUTH about Coronavirus
- Corona virus is here, are you ready? (Learn how to survive)
- Get your coronavirus supplies while they last

Canadians are encouraged to take some simple steps to protect themselves, not just during the COVID-19 isolation period, but at all times.

What steps can companies take to ensure that their workers are better protected from these cyber-hackers? How can individual employees protect themselves? Some recommendations are below.

Companies should ensure that their employees use only company devices (not their personal devices) that access company networks using secured VPNs (virtual private networks) or other secure portals. Company networks should only be accessible using multifactor authentication. Organizations should promptly deploy all required security patches and updates to their critical enterprise software as well as implement current anti-virus or anti-malware software on computers and networks.

Computers, router firmware, and web browser software should be kept up-to-date and legacy software should be replaced with currently supported versions. Companies should ensure that access to sensitive documentation is limited to only those who especially require access, and all employees should receive basic cybersecurity training, reinforced through internal policies and periodic testing.

Companies should advise their employees not to download confidential proprietary documents onto their personal devices, and employees should be required to use sophisticated passwords (plural) that are different from those for their personal/home accounts.

As busy as they are trying to keep the lights on, companies should periodically remind their employees about these increased risks during this pandemic, including being on the lookout for not-so-obvious phishing attempts.

Individual employees should recognize that they have a responsibility to be especially vigilant now, given the incredible increase in coronavirus scams, and practise safe computing. As recommended by the CCC, users should ensure that the address or attachment is relevant to the content of the email in order to protect against malicious email. It's critical to take the time to make sure that you know the sender of the email and that the email is legitimate; typos are a dead giveaway they are not. No one should open email attachments that come from sources they are unsure of.

To protect against malicious attachments, employees should ensure the sender's email address has a valid username and domain name, and should be extra cautious if the tone of the email seems urgent or is otherwise off. It doesn't hurt to verify an unexpected email with an attachment with the supposed sender. Remember that so-called critical or important information that comes via attachments or hyperlinks may also be scams.

To protect against malicious websites, make sure the URLs are spelled correctly. It's safer to directly type the URL in the search bar instead of clicking a provided link, but if you must click on a hyperlink, hover your mouse over the link to check if it directs to the right website; and try to avoid clicking on links in email addresses that direct you to log into a website. Take the time to search and find the login page yourself using your own web browser, and log in that way.

If you intuitively think there's a reason to question the legitimacy of a message that you receive, it's better to simply ignore it, or contact the supposed sender to verify it. Do not respond to requests for sensitive information, including to update account payment information.

Lastly, if you make a mistake and fall for these scams, you are only human. But if your errors have resulted in the unauthorized disclosure of personal information or confidential information, you or your organization may have triggered mandatory data breach reporting requirements under various provincial and federal Canadian/international laws, as well as other regulatory reporting requirements.

Be careful out there, and stay safe!

This article was originally published in Canadian Lawyer magazine.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.