Planning Matters

Leith Wheeler
INVESTMENT COUNSEL LTD.

Quiet Money®

Contributor:
James Goodchild
Chief Information Security Officer
Chief Technology Officer
Leith Wheeler Investment Counsel Ltd.

Editor:
Mike Wallberg, CFA, MJ
VP, Marketing & Communications
Leith Wheeler Investment Counsel Ltd.

Visit our website, leithwheeler.com, to download previous Newsletters and read our latest Insights.

SPRING **2021** EDITION

How to Protect Yourself from a Cyber Breach this Pandemic

A common tactic of the hacker is to create a sense of urgency, to get people to react to their message without pausing to question what's being asked of them. A pandemic provides a built-in sense of that urgency, so the past year has unfortunately created many new opportunities for those seeking malicious gain to target both individuals and businesses. Awareness of the tricks and a few simple steps can help protect you.

Common Cyber Breach Techniques

Playing on Your FOMOOV (Fear of Missing Out on Vaccines)

Take the vaccine, for example. Hackers impersonating legitimate health authorities have sent out messages with links asking people to "Act fast and register now" for their vaccine, noting that supplies are limited. This can result in individuals frantically

trying to book their vaccine without thinking to check the validity of the email. And of course, in that scenario it will seem quite reasonable to provide details such as your name, birthday, and government-issued health insurance number, which all help the hacker create an identity using your information, or leverage the information to compromise your financial health in other ways.

Exploiting Government Assistance Programs

Hackers are leveraging the COVID-19 pandemic to engage and ask individuals in need to apply for the Canada Emergency Response Benefit or Canada Emergency Student Benefit programs. This is, of course, a scam, and the information you provide will help the hacker achieve their goals of applying for the program in your name with the payments directed to their accounts.

As a matter of note, the Canadian government does not reach out via email or text to ask individuals to apply for assistance programs. Hackers have also posed as government employees asking for money back, because of some (fabricated) issue with the assistance request.

Wedging into the Gap in Electronic Business Transactions

Another security challenge created by the pandemic is the fact that more business transactions are now conducted remotely, and, in some cases, businesses have not adequately prepared themselves for the challenge.

Prior to COVID-19, it was common for businesses to require you to come down in person to register for their services, or at a minimum, require a "wet" or ink signature, especially if money was involved. With companies now moving to electronic confirmations, hackers can remotely register for services using your identity if they have acquired enough of your personal information and if the business does not have the proper checks in place. This can leave you on the hook to cover the costs of those services.

Vishing

A common hacker tactic at this time of the year - tax season - is to use vishing, or voice phishing. Using an automated, randomized dialing program, hackers will place a call with a recorded voice advising you that Revenue Canada has discovered an issue with your tax filing, that you owe money, and that you must immediately contact them to prevent legal actions. The message will provide you a call back number to arrange payments. This phone number belongs to the hacker. If you call them, they will typically ask you to confirm your personal information – which they can use to build identities – and ask you to pay your outstanding tax bill immediately, preferably with Bitcoin or a similar non-traceable service. Another popular vishing campaign purports to be from Service Canada and asks the victim to act immediately or face legal consequences.

The Canadian government does not reach out via email or text to ask individuals to apply for assistance programs.

Protect Yourself Against a Cyber Breach

Double Check the Source and Content of the Message

As a general note, whether it is an email or a voice call, if the message is unsolicited and demands immediate action, do not respond using the information provided in the message, even if the message appears to come from someone you know. Instead, call the person, company, or agency using contact information on file or by looking up the phone number and ask if they have tried reaching you regarding the topic in the message.

Should you receive an unsolicited message that appears to be from a friend, client, or peer asking you to click a link or open an attachment, it may seem a prudent action to reply to the sender asking if the link or attachment is safe. Beware! Since the original sender's email was compromised, it would then be the hacker replying that the link or attachment is safe.

If the unsuspecting individual then clicks on the link or opens the attachment, what happens next? Their computer may start acting up, or their email account may start sending emails containing the same compromise to all their contacts. If the individual reuses the same password on multiple services, especially banks, they may find fraudulent charges suddenly appearing on their statements.

The Importance of Security Training, Especially for Employees

Analysis from entities like the RCMP, FBI, and the Ponemon Institute all agree that the most common way companies are compromised is through a directed attack against employees. Employees are the weakest link in a corporation's security program unless they have been trained to look for security anomalies.

Industry metrics suggest that without training, the likelihood of an individual falling for a targeted phishing campaign runs around 25%. That number falls to about 2% after they go through security training over the course of one year. Security training services for corporations are generally inexpensive and many of them have interactive videos with metrics to help organizations measure the effectiveness of their program. Most service providers also offer ethical phishing campaign capabilities so the corporation can test employees by sending out an authorized phishing test. The tools provided make creating these ethical campaigns easy. **Leith Wheeler employees all undergo regular cyber security training to help ensure our systems and client data remain more secure.**

Regardless of how a corporation decides to approach it, cyber security education is key to reducing security risk for the organization. In fact, many organizations have implemented security training awareness regimes for their board or executives, so that they understand the risks and liabilities their firms have if a security breach occurs.

Reporting Cyber Fraud

If you do believe you are the victim of a cyber security compromise or believe you have discovered a fraud, the Canadian government asks that you report it. You can do so by clicking on this link to the Government of Canada's Canadian Anti-Fraud Centre. (You can trust us on this one!)

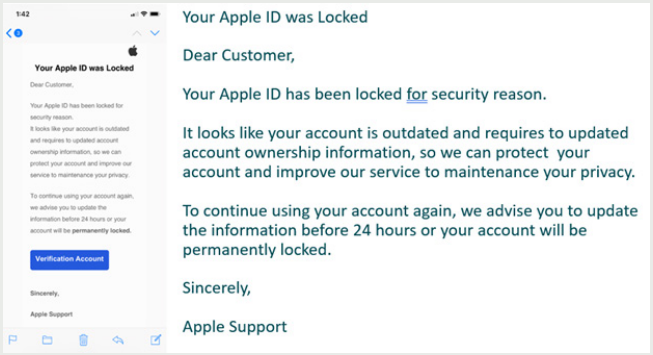
Leith Wheeler and Cyber Security

While no security program is 100% effective, at Leith Wheeler we have taken steps to implement an enterprise cyber security program that educates employees, reduces corporate risk, and improves the overall security posture of the company. Cyber security is a community activity and each of us need to be participants.

As part of that planning, we have developed a cyber security incident response plan, which includes typical scenarios that the company might encounter, default responses, and contact information for legal, insurance, authorities, and any applicable regulatory bodies that need to be contacted. If a cyber security incident does occur, the plan can be referenced to ensure no steps in the response are missed and the legal exposure, corporate risk, and reputational impacts are minimized.

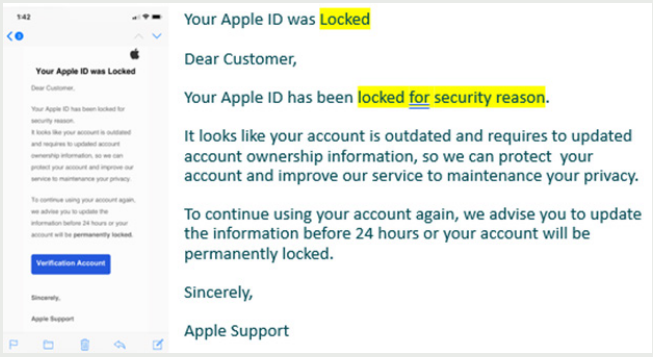
Case study: *Phishing Email*

In parting, you will find below an actual phishing email captured for illustrative purposes. The small column on the left is the email as it shows on an iPhone and the column to the right is the same text blown up to a size where it is easily readable. Can you spot the hints that this is a phishing email?



Here are just a few hints (there are others to spot!):

- Odd capitalization of "Locked" in the first sentence
- "Locked for security reason" is not gramatically correct - and here you thought elementary school grammar classes were a waste of time!



Contributor

James Goodchild joined Leith Wheeler in 2019 after eighteen years at Greystone Managed Investments where he held numerous roles including Chief Information Security Officer and VP of Technology. He is responsible for security and technology at Leith Wheeler. James has been in the financial sector since 1994 and has a number of technology designations. James has also worked briefly worked in the Health sector as a Chief Security Officer and in the Construction sector as an estimator and project manager.

Vancouver Office
Suite 1500 400 Burrard Street
Vancouver, BC V6C 3A6
Tel: 604.683.3391
Fax: 604.683.0323

Calgary Office
Suite 570 1100 1st Street SE
Calgary, Alberta T2G 1B1
Tel: 403.648.4846
Fax: 403.648.4862

Toronto Office
Suite 1801 145 King Street W
Toronto, Ontario M5H 1J8
Tel: 416.646.8240
Fax: 416.646.8249