DECEMBER 2019 VOL. 3

CYBER MONDAY

A monthly cyber-security and data privacy bulletin from the UGDSB

VULNERABILITY MANAGEMENT

Data is the New Oil

School districts, hospitals and municipalities have increasingly become the victims of cyber criminals. The frequency and ease of access to sensitive information, makes us vulnerable to attacks from hackers.

How secure are your passwords, really?

The average Canadian has over 100 secure accounts that require passwords. Many have just given up, re-using a few passwords over and over again. What can you do?

- Increase the length of your password. 12 characters (upper and lower case, numbers and special characters).
- Use a favourite phrase or line from a book you like
- Use different passwords for each critical service you access
- Do not use your work password(s) for non-work accounts

IN THIS ISSUE

PHISHING, SPEAR PHISHING & RANSOMWARE

Phishing & Spear Phishing

The average office worker receives 90 emails a day. This volume of emails makes us vulnerable to phishing attacks. Phishing is a form of fraud designed to trick a user into thinking they are receiving message from a reputable entity or person. A phishing email will include malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims. While a phishing attack sends mass emails to as many people as possible, a spear phishing attack targets a specific person or company. Hackers research their target to increase their chances of fooling a victim. 91% of successful data breaches start with a spear phishing attack.

Tell-tale clues of a phishing scam

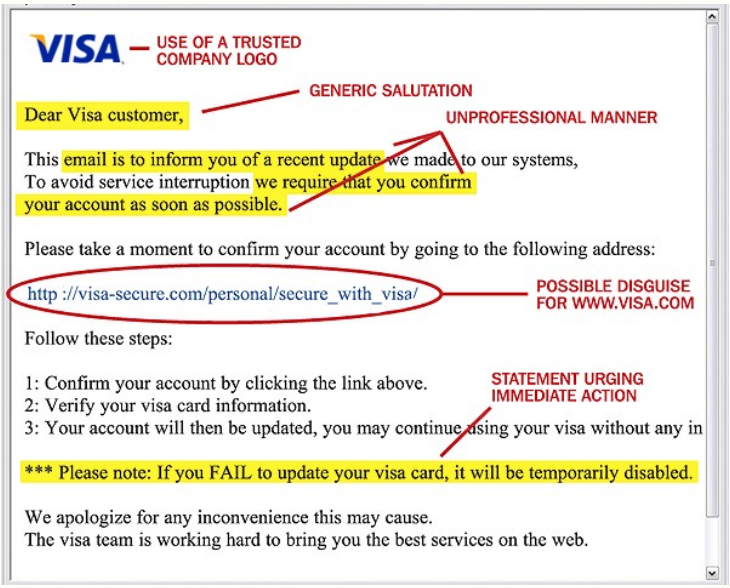
- Sender's email address is unfamiliar or unusually complex
- Content of the message conveys a sense of urgency, for example your account has been compromised you are in legal jeopardy
- Requests to validate or update your account information by clicking on a link

Ransomware

Hackers commonly use phishing attacks to introduce ransomware into a company's computer network. Once installed on even one computer, ransomware infects an entire network locking everyone out of their files. Affected companies must decide to pay a ransom or try to recover their files, a process often more expensive than paying the ransom.Ransomware attacks are increasingly common in Canada. In the past year multiple public agencies in Canada have been hit by ransomware attacks including:

- City of Stratford - April, 2019
- Eastern General Hospital, Toronto - September, 2019
- City of Woodstock - September 2019
- Territory of Nunavut - November 2019

Sample Phishing Email



PROTECT YOURSELF AGAINST EMAIL PHISHING SCAMS

- Do not click any links or download any attachments in a suspicious email.
- Hover your mouse over the link or button in the body of the email to see the actual url.
- Contact the company directly by phone to inquire rather than using any link or other contact information provided in the email.
- Do not forward the email to anyone or reply to the sender.