Common Cyber Threats

Cyber Security Tips

The purpose of this risk management document is to help credit unions with definitions, examples and prevention tips for common cyber threats and attacks. This document reviews:

- Malware;
- Phishing;
- SMShing;
- Business E-mail Scam;
- Ransomware;
- Pharming; and
- Man-in-the-middle Attacks.

Employees are a Credit Union's Best Defence

Educating credit union employees and engaging them in cyber security is crucial in trying to successfully fend off cyber threats and breaches. Employees of an organization are regularly targeted as fraudsters look to exploit human error, one of the easiest ways to gain access to your devices, networks and information. Investing in employee education is investing in one of your most important lines of defence.

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, ransomware and adware.

Example: Fraudsters send spam e-mails, trying to trick their victims into opening a malicious e-mail attachment. When the attachment is opened, malware becomes embedded into the victim's computer. This malware begins to harvest information from the computer that will later be used for fraud and identity theft.

How to Protect Yourself and Your Credit Union:

- **Never click on links or download files / attachments from unknown sources or senders.**
- **Be cautious when downloading free software ("freeware" such as games, applications, programs, etc.) from the internet. Malware can be embedded in these free downloads. Research the "freeware" before downloading.**
- **Keep your computer, phones and software updated. Always use an anti-virus program and keep it updated. These updates close exploits and help protect against the latest versions of malware.**

Phishing

An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking a usually well-known brand, usually for financial gain. Phishers attempt 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

The term "Spear-Phishing" is used when a specific individual is targeted to be exploited; the attack is tailored to this individual.

Example: Fraudsters send out mass e-mails to potential victims, imitating a well-known financial institution. The e-mail asks the recipients to click on a link provided within, where they are asked to enter personal banking information. The fraudsters collect and record their victims' information, gain access to their online banking and fraudulently e-transfer money out of the victims' accounts.

How to Protect Yourself and Your Credit Union:

- **Legitimate financial institutions will never contact you by e-mail and ask you to provide your online banking credentials.**
- **In general, never provide personal information when contacted by unsolicited e-mails.**
- **Don't accept e-mail money transfers from unknown parties or when you aren't expecting a transfer.**

SMShing

A form of “Phishing” that targets mobile phones. Fraudulent SMS messages (text messages) are designed to induce users to reveal personal or financial information via the mobile phone.

Example: Many of these SMShing attacks are very similar to e-mail phishing. You receive a text message on your cellphone from an unknown number. The sender of this text is claiming to be a financial institution and has provided a link, asking you to sign into your account. The banking information entered is collected for fraudulent purposes.

How to Protect Yourself and Your Credit Union:

- **Legitimate financial institutions will never contact you by SMS (text message) and ask for you to provide your online banking credentials.**
- **Never reply to text messages from unknown senders. The fraudsters may be charging you very expensive text messaging fees.**

Business E-Mail Scam / CEO E-mail Scam

Criminals use this scam to trick employees into electronically transferring large sums of money to fraudulent accounts.

Examples:

- Criminals compromise or imitate the e-mail account of a credit union manager or employee of the credit union. The criminals use this hijacked or imitated email account to direct credit union staff to wire transfer money to an unknowingly fraudulent account.
- Creating fraudulent invoices that appear to be from your credit union’s usual and legitimate vendors / suppliers. These fake invoice requests will ask for the wire transfer payment to be sent to an alternative account which belongs to the criminals.

How to Protect Yourself and Your Credit Union:

- **Require all staff to verbally confirm all internal wire transfer requests. Encourage this practice even if the request appears to originate from a high-level credit union employee or manager.**
- **Call vendors and suppliers to confirm the legitimacy of invoices that require payment by wire transfer, especially if a new account number is requested. Make sure staff call the phone number from your file, not from the invoice provided.**

Ransomware

Software that denies you access to your files until you pay a ransom.

Example: A victim has clicked on a link in an e-mail from an unknown sender. A pop-up appears on the victim's screen notifying them that their computer is being held hostage. A hacker has blocked access to all programs and files with the use of encryption, and won't release the computer until a bitcoin ransom fee is paid.

How to Protect Yourself and Your Credit Union:

- **If you believe you have become infected or are in the process of being infected by ransomware – power off your device (physically hold the power button down). Immediately call your credit union's IT or Security Department to receive further instructions.**
- **Do not click untrusted links in emails or pop-up ads – remain vigilant.**
- **Ensure you have a backup of your recent important files and test their recovery.**
- **Ensure you have recently applied all your updates on all computers and personal devices.**

Pharming

Redirecting users from a legitimate website to a bogus copy, allowing criminals to steal the information users enter.

Example: You have been forwarded a webpage from a reputable online retailer. The website looks legitimate, but a fraudster has created a very convincing replica. The intent of the website is to collect credentials, plastic card information and banking information when you go to checkout for the items you have "purchased" (but won't receive).

How to Protect Yourself and Your Credit Union:

- **Look at the URL (website address) when putting personal information into websites. Check to see if the name of the company is spelt correctly or if there are any additional characters in the website address.**
- **A website's URL should start with "HTTPS" (versus "HTTP") when you are prompted to enter personal information. The "s" means the website is secure. You may also look for a padlock icon which also indicates that website uses encryption security.**

Man-in-the-Middle Attacks

A man-in-the-middle attack reroutes a communication between two connections, for the purposes of monitoring, stealing or altering the information.

Example: You go to a local coffee shop for a break from work. At the coffee shop you sign into their free public wi-fi and decide to log into your online banking and check your account balance. This public wi-fi has been compromised by fraudsters though, who are stealing online credentials by picking up confidential information as it transmits through the internet network.

How to Protect Yourself and Your Credit Union:

- **Use a VPN (virtual private network) when logging onto public wi-fi connections. Ask your credit union security team about the use of VPNs.**

Get Cyber Safe Canada

Many of the definitions used for the cyber-attacks above were adapted from the Government of Canada's "Get Cyber Safe" website. This website is a great resource for consumers and businesses to improve their cyber security, practices and overall awareness.

Click here to visit the Get Cyber Safe website.