HOW TO USE ONLINE BANKING SECURELY

SEPTEMBER 2020 ITSAP.00.080

Online banking offers you the convenience of accessing your financial information through a mobile device or a computer. Although your online banking services should be secure (e.g. using authentication and encryption), there are risks related to the possibility that threat actors can find ways to access your sensitive information. This document includes some tips on how you can protect your sensitive financial information while using online banking services.

HOW IS ONLINE BANKING USED?

Online banking can be used to complete many tasks, including:

- Checking your bank account balance and statements
- Paying your bills
- Depositing cheques
- Transferring funds to other accounts
- Managing your accounts
- Setting up automatic transactions

A financial institution may offer different services depending on how you are accessing your online accounts (e.g. mobile device or desktop system).

WHAT ARE THE RISKS?

Although online banking is generally safe, there are ways that threat actors can gain access to your sensitive information. Commonly, threat actors use phishing attacks and malware.

PHISHING ATTACKS

A threat actor tries to trick you into sharing sensitive information by texting, emailing, or calling you and pretending to be a trusted source (e.g. your bank).
For example, a threat actor claims to be a representative from your bank, notifies you of unusual activity related to your account, and asks for sensitive information, such as your account or credit card numbers. A threat actor may also send an email with a disguised link that redirects you to a fraudulent website that directs you to enter sensitive information (for "verification").

MALWARE

Malware (i.e. malicious software) is designed to infiltrate or damage a computer system. If your device is infected with malware, a threat actor can collect your sensitive information and gain access to your accounts, such as in the following example methods:

- Phishing messages include attachments and links that are disguised as your banking services to trick you into downloading malware onto your device.
- Fake banking and money transfer applications collect your banking credentials to access your sensitive information.

There are many threats to look out for when using online banking. But by learning how to identify common cyber threats, you can be better prepared and protect yourself. For more details on how to avoid phishing attacks and malware, see *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks* and *ITSAP.00.057 Protect Your Organization from Malware,* which are available on **cyber.gc.ca**

AWARENESS SERIES

HOW CAN I PROTECT MY ONLINE BANKING INFORMATION?

There are ways you can reduce the risks associated with online banking. Review the list of cyber security **Do's** and **Don'ts** for protecting your bank account, sensitive information, and money from cyber criminals.

DO

- **Read and understand your bank's terms and conditions** to understand your responsibilities as the account owner and the responsibilities of your bank.
- **Lock your devices with a PIN** to secure it if lost or stolen.
- **Use a strong passphrase or password for your account**. For more details on passwords and passphrases, see *ITSAP.30.032 Best Practices for Passphrases and Passwords* on our website.
- **Use multi-factor authentication** (such as a fingerprint and a passphrase) to provide an extra layer of security in case your passphrase is compromised. Learn more about multi-factor authentication by reading *ITSAP.30.030 Secure Your Accounts with Multi-Factor Authentication*.
- **Install a firewall and anti-virus software** on your computer to protect yourself from cyber threats, such as malware.
- **Update and patch your device and software** to repair security vulnerabilities and issues. For more details on the importance of updates, see *ITSAP.10.096 How Updates Secure Your Device on* our website.
- **Use your carrier provider service or a secure Wi-Fi network** to protect yourself from accidentally using spoofed Wi-Fi portals (e.g. threat actors disguised as a coffee shop's network).
- **Access your bank's website or download the bank's app only from legitimate sources** (e.g. certified through an encrypted source [https] and company owned) to protect your data from threat actors who create fake websites or apps.

DO NOT

- Share your credentials with anyone (e.g. in person and online), even your family members.
- Store your credentials (e.g. password managers, "remember me" option, device notes), as this risks having your credentials stolen (e.g. lost or stolen device, malware).
- Use personal information (e.g. birthdate, address, pet's name) when creating passphrases, passwords, or answers to security questions. Threat actors can gather these personal details from your social media accounts.
- Use a public computer to access your bank account.
- Click on links or attachments in emails or text messages without confirming the sender's details.

WHAT IF I FALL VICTIM TO FRAUD?

If you have fallen victim to fraud or attempted fraud, contact your bank immediately to lock your account. Your bank can help you manage risk by resetting your account credentials.

Report the incident to the Canadian Anti-Fraud Centre at 1-888-495-8501 or online at antifraudcentre.ca.

Need help or have questions?
Visit the Cyber Centre website at **cyber.gc.ca**