Online Banking Security Guarantee

In the unlikely event that you experience a loss resulting from a transaction through online or mobile banking that you did not authorize, we offer an **Online Banking Security Guarantee** for account losses, provided you have met your security responsibilities.

Member Security Responsibilities

To ensure that you are doing your part in protecting yourself from online cybersecurity fraud, you are responsible for ensuring the following:

1. Use of a Firewall

   Windows has a firewall already built in and automatically turned on.

2. Up-to-date Operating Software

   One of the most common ways that hackers target people is by exploiting vulnerabilities in outdated software. Outdated software risks can leave you open to a variety of hacks, including ransomware, malware, data breaches, and more. To ensure that your computer operating system is up to date, turn on automatic updates in Windows Update to keep Windows, Microsoft Office, and other Microsoft applications up to date. Additionally, turn on automatic updates for non-Microsoft software, especially browsers, Adobe Acrobat Reader, and other apps you regularly use.

3. Use of Antivirus Software

   If you run Windows, you have Windows Security or Windows Defender Security Center installed on your device.

   Tip: If you're a Microsoft 365 Family or Personal subscriber, you get Microsoft Defender included with your subscription at no extra charge. It helps protect all your devices - Windows, Mac, Android, and iOS. For more information, see Getting Started with Microsoft Defender.

4. Use Strong Passwords

   To be covered under our Online Banking Guarantee, implemented minimum best practices when it comes to passwords is mandatory for all members. Strong passwords are key to mitigating Online and Mobile Banking and Brute Force losses. Password length is a primary factor in characterizing password strength. To strengthen the security of your online information, ensure your passwords are a random mix of at least 8 to 16 characters, including letters (upper and lower case), numbers and special characters.

   - Never write your passwords down; instead, you should memorize your passwords or use a password storage tool such as LastPass™.
   - Never share your passwords! If someone needs to support you with your banking, you can make arrangements with the Credit Union to add them to your account, and they will be provided with their login details to MDI.

5. **Don’t Open Attachments or Click on Suspicious Links**

   The general rule of thumb is not to open any email attachments, unless you’re absolutely sure they’ve (a) come from a trusted contact; and (b) you know what they are. Security software should catch most malware that arrives by email attachment, but it’s not infallible. Furthermore, do not click on links that appear in Social Media Posts, Online Ads, Facebook Messenger, etc.

6. **Browse The Web Safely**

   Gambling, adult content and illegal (pirated) software sites are all popular with hackers because they make it easy to spread malware placing you at increased danger of falling victim to computer viruses. Many of these sites install malware on the fly or offer downloads that contain malware. If you must go to these at-risk sites do the following:

   - Use a modern browser like Microsoft Edge, which can help block malicious websites and prevent malicious code from running on your computer.
   - Check the site security. When visiting a new site for the first time you should pay close attention to their security. Fortunately, this is much simpler than it sounds. As you click through to the checkout, take a look at the browser’s address bar. Does the address begin https? Is there a little padlock icon? If the answer is yes, all traffic between your computer and the website is encrypted so that no one can steal your data.
   - To check how trustworthy the site is, click on the padlock icon and look at the certificate details. If the certificates type is listed as “extended validation”, you know that the site belongs to the company – and is fully legitimate.

7. **Do Not Use Public WIFI**

   Never use public WIFI to access sensitive websites such as your online banking. Cybercriminals can use unsecured Wi-Fi networks to spread malware to other devices on the network — especially if those devices aren't up to date.

8. Don't use USBs or External Hard Drives Unless You Own Them

To avoid infection by malware and viruses, ensure that all external devices either belong to you or come from a reliable source. Because USB cables can transfer both power and data, so-called juice-jacking is relatively straightforward. Hackers load malware (like a virus) into USB power outlets at airports, hotel lobbies, or cafes. When an unsuspecting user plugs their device into the outlet directly with a USB cable, that device can become infected.

Next Steps If You Suspect Your Computer Has Been Hacked

- If you suspect that your computer or phone has been hacked. Immediately change your passwords related to how your access your computer, email, online banking, and any other online accounts you may have such as CRA, Amazon, Facebook, Instagram, etc.
- Log out of all online accounts and disconnect from the internet.
- Take your computer to a reputable service provider who will use various diagnostic tools to detect and eliminate malware and computer viruses.

If You Have Incurred Financial Losses Through On-Line or Mobile Banking

- You must promptly, within 24-hours, report any financial losses that you believe result from cybercrime to the Credit Union.
- For us to place a claim with our Cybersecurity Insurer, a diagnostic must be performed on all devices that you use to access online banking, and the provider of the diagnostic testing must attest that you have been operating your computer with an up-to-date operating system and have malware and antivirus software installed.
- All insurance claims to cover losses as a result of Cybercrime must be accompanied by a police report that you, the member, filed when your funds were stolen via Online and Mobile Banking. This is a mandatory requirement before reimbursement.