financial backup for life.

Online Security

Internet banking provides convenient access to your accounts and the ability to perform transactions from home, work, or other locations. However, it's important to remember that when you connect online, your device can also be exposed to other users, software, or potential threats.

Without proper protection, an unknown party or virus may be able to access your device in a very short time. To help keep your information secure, we recommend:

- Keeping your operating system and software up to date
- Installing trusted antivirus and anti-malware programs
- Using strong, unique passwords
- Avoiding public WiFi when accessing online banking

Protecting your device helps protect your personal and financial information.

How We Protect Your Security

We take many precautions to safeguard the online banking environment and to ensure your information remains secure. Our Online Services provider Central 1, in collaboration with Intellect Design Arena delivers industry-leading security so that your personal and financial information is protected while in transit between your computer and our server.

This is achieved through the use of industry standard encryption (TLS), an industry-standard technique that scrambles data using complex mathematical formulas. Encryption ensures that information cannot be read or altered while in transit. (Some browsers may create a more secure channel than others depending on their encryption strength.)

Additional measures we use to protect your information include:

- **Strong PAC - Personal Access Code (PAC):** Requires Members to use a stronger password with a minimum of 8 to a maximum of 30 characters including capitals, numbers and symbols. Only individuals who provide a valid PAC can access account information.
- **Increased Authentication with 2 Step Verification: A**a security feature that strengthens online and mobile banking security by using a step-up authentication during higher-risk activities.
- **Automatic logout:** For added protection, your online banking session will automatically end after 15 minutes of inactivity.
- **Strict database security:** Access to our systems is carefully managed to prevent unauthorized entry.

Your security is our priority, and we continue to monitor and update our systems to keep your information safe.

financial backup for life.

Protecting your personal access code (PAC).

Just as you play a vital role in protecting your home and possessions, you also share responsibility in protecting your personal information. To ensure that only you can access your accounts, we use your Personal Access Code (PAC) as your secure "key" to online banking.

It is your responsibility to keep your PAC safe. Please follow these important security practices:

- Choose a PAC that is not easily guessed
- Your PAC must be **8–30 digits** long, including capitals and numbers.
- Keep your PAC confidential — never share it with anyone.
- Do not write your PAC down or store it on your computer.
- Never disclose your PAC in an email, voice message, or phone call.
- Ensure no one can see you enter your PAC.
- Change your PAC regularly — we recommend every **90–120 days**.

Your PAC is the key to your account security — protect it just as you would the key to your home.

Protecting Your Device

We provide a secure channel for Members to communicate with us. Once information reaches your computer or device, it's up to you to keep it protected. Here are some important steps you can take to safeguard your information:

- **Always log out** of Online Banking using the logout button, and close your browser if you step away from your computer. Browsers may retain information until they are fully closed.
- **Clear your browser cache** regularly. Browsers often store information in unprotected files to improve performance. Use your browser settings or computer utilities to erase these files.
- **Disable "save password" features** in browsers and software you use to access the Internet.
- **Use antivirus software** and keep it updated. New viruses appear daily, so update definitions weekly. Always scan downloads, programs, email attachments, and only accept files from trusted sources.
- **Install a personal firewall** to prevent others from accessing your computer over the Internet.
- **Apply security updates** for your operating system and browser as soon as they are available.
- **Run anti-spyware software** and scan your computer regularly.

By taking these steps, you'll help ensure your personal and financial information stays secure.

Protecting Yourself from Electronic Identity Theft

Electronic identity theft can occur when someone responds to a fraudulent email asking for personal banking information. With this information, criminals may be able to access your accounts, open credit, make purchases, or borrow money in your name.

You can help protect yourself by following these precautions:

- **Remember:** We will **never** ask for your passwords, PIN, or login details by email.
- **Check the web address** on any page that asks for account information. Legitimate online banking sites always begin with **"https"** in the address bar.
- **Look for the padlock icon** in your browser. By clicking it, you can view the site's security certificate. Fraudulent sites will not have valid details.
- **Type our web address yourself** to be sure you are connecting to our server — avoid using links in emails.
- **Review your statements regularly** to confirm that all transactions are legitimate.

Staying alert to suspicious emails and websites is one of the best ways to protect your identity and your accounts.