Secure Digital Banking

Our digital banking platform is designed to make accessing and managing your finances convenient, intuitive and secure.

We also advise you take additional precautions while browsing online and practice good cyber hygiene like strong passwords, safe browsing and regularly monitoring your accounts.

Let's work together to protect your account and keep your money safe.

Our security protections

Our digital banking system has industry-leading security capabilities, including robust fraud prevention, cyber security features and high-risk transaction protections to ensure that your transactions are secure while data is transmitted between your device and our banking server.

Encryption

We use 256-bit TLS encryption on our desktop website and mobile app, enabling you to easily and securely complete banking transactions on your phone, tablet or computer.

Controlled account access

You have control over your account access – only you know your sign-in credentials, user name and password. Our employees do not have this information, nor do they require it from you.

Password protections

There is a maximum number of attempts to input the password for your account. If it exceeds the number, your online access will be disabled, and you must contact a member representative to assist you.

Protect yourself

- Do not provide account or personal details in an email, as it's not secure. Our credit union will never ask for this information through a communication.

- Do not follow links from e-mails to your financial institution's website. Type in the address and look for https in the address.

- Scammers will try scare-tactics – saying your account has been closed or there's an issue to get you to take immediate action. Call your credit union to independently verify these types of messages.

Use strong, unique passwords

- Ensure your banking login password is unique – avoid re-using passwords from other sites and services you use.

- Choose a password that is memorable for you, but not easy to guess, and avoid using personal information like phone numbers, birth dates, your pet's name, etc.

- Don’t use the auto-save function for user names and passwords on your browser and device. Consider using protected password management software or another secure system for storing passwords.

- Never share your password with anyone – including employees at this credit union. They will never ask you for your credentials.

Monitor your accounts

- Review your statements regularly and set up transaction alerts for your account to help you identify any irregular activities.

- Our alert messages will never contain any personal information about you or account and will never ask you to click or download anything.

Be aware of cyber crime

- Cyber-criminals seek vulnerabilities in human behaviours to steal credentials. They are using social engineering tactics to trick people into providing sensitive information or visiting a malicious website. Below are some of their tactics:

- Financial phishing and smishing scams: A cyber-criminal poses as your financial institution sending you emails (known as phishing) or text messages (known as smishing) in an attempt to get you to provide your login credentials.

Protect your computer

Threat protection software secures your information and privacy on your computer. Installing this software will mitigate virus threats, ransomware, provides firewall protection and protect you from harmful sites and data.

Browse safely

- Make sure you are using the most current version of your online browser, and it’s shows https:// as part of the web address in the browser bar, as this verifies the security certificate of the website is authentic.

- Sign out of your online banking session

- Don’t access your account using public Wi-FI or a public computer

- Use our alerts options and one-time password features

Manage your operating systems

Keep your operating system up to date to protect against malware and viruses and download the latest security patch when it becomes available.

Protect your device

- Keep your operating system updated and install anti-virus software
- Ensure your device has password protection
- Download apps exclusively from Google Play, Apple Store, etc., not from a link
- Install anti-virus software for your smartphone if available and update it frequently
- Install an app that enables you to track the location of your device. These often enable you to remove locate or factory reset a device if lost or stolen
- Keep your smartphone's operating system updated
- Don’t remove the manufacturer’s restrictions on the device (aka jailbreaking)