BEST PRACTICES

Our goal is to help you protect yourself from online fraud. It is important that you have effective cyber security practices in place to safeguard your personal information.

BEST PRACTICES ON HOW TO PROTECT YOUR ACCOUNT

- Monitor and reconcile your accounts frequently especially if you shop online.
- Effective cyber security practices include clearing the internet browser’s temporary history files before visiting the financial institution’s website, and educating yourself on how to avoid having malware installed on a computer.
- Never leave a computer unattended when using online banking and always lock your computer when you have logged off.
- Immediately report any suspicious activity in your accounts to Credit Union personnel; there is a limited recovery window and a rapid response may prevent additional losses.
- To guard against computer viruses and malware, do no click on email attachments or internet links unless you know and trust the source of the email.

SAFEGUARDING PERSONAL INFORMATION AND PASSWORD

- Never share login IDs (User IDs), passwords or PIN numbers.
- Do not use the login or password for your financial institution on any other website or software.
- Use strong complex passwords (upper, lower, numbers and special characters).
- Do not write down your login ID or passwords. If you do, store the information in a secure place.
- Never access your financial institution’s website for online banking from a public computer at a hotel/motel, library or public wireless access point.
- Don't provide personal or financial information over unsecure websites.

SAFER COMPUTING

- Firewalls and anti-virus software can protect your computer.
- Be on guard against questionable web sites and email scams requesting you to disclose sensitive personal or financial information.
- Ensure your anti-virus software is kept up to date.
- Turn off your computer when you’re not using it, even if you have antivirus and firewall software.
- Be aware that credit unions and other legitimate businesses never email members asking for passwords or updated information.
- Never click on a link in a suspicious email. Instead, confirm the Web address on your own, and then type it directly into the browser window.
- When making an Internet purchase, before entering any personal or payment card information, ensure that the merchant site is secure by noting the web address (URL) says https://
- Change passwords and PINs periodically.