



## Online Banking Security

Emerald Credit Union is committed to protecting your personal information. Our Online Banking system uses several different measures to ensure your information is protected. All information within our Online Banking uses the Secure Socket Layer (SSL) protocol to ensure that your transmitted account information is protected. All information transferred through Online Banking has a 256-bit encryption which makes your information unreadable as it passes over the Internet. Other online security measures include: automatic time out that occurs if there is no activity within the required time period, recognizing the user's computer and usage patterns, limited log-in attempts, challenge questions and security phrases.

As we move forward in this digital world it is important that you take your own security measures to ensure your information remains protected.

Here are some tips on how to stay safe:

- Never give out any personal information including user names, passwords, social security number, or date of birth.
- Don't respond to email, text, or phone messages that ask for personal information. Legitimate companies don't ask for information this way.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- Always check your account and credit card statements for any unusual activity. If there is any unexplained transaction activity, report it as soon as possible.
- Keep your debit and credit cards in a safe place. We recommend carrying the minimum number of debit and credit cards as possible. Cards that are not carried with you should be kept in a secured location.
- Never give your Personal Identification Number (PIN) number to anyone.
- When using social networking sites, be sure to use the strict privacy policy settings.
- Don't use personal information for your user names or passwords, such as birth dates or social security numbers.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address: the "s" stands for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus, anti-spyware software, and a firewall on your computer.
- Set your computer's operating system, web browser, and security system to update automatically.