



INTERNET HOME BANKING AND ONLINE SECURITY

Safeguarding Your Information Online

In today's high tech world, we are able to do things more quickly and conveniently electronically whether it is to send a letter via email, pay bills or even go shopping online. With this increase in speed and convenience also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At Windsor Lock Credit Union, the security of member information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid fraud is to become an educated consumer and we would like to help you in this endeavor. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

How to Keep Yourself Safe in Cyberspace

An important part of online safety is knowledge. The more you know, the safer you'll be. Here are some great tips on how to stay safe in cyberspace:

- 1. Set good passwords.** A good password is a combination of upper and lower case letters and numbers and one that is not easily guessed. It should contain at least 8 characters including numbers and a mixture of capital and lower case letters. Don't use your account number or social security number. Change your password frequently. Don't write it down or share it with others.
- 2. Change your User Name.** If your user name is your account number, change it to a more secure choice.
- 3. Don't reveal personal information via email.** Emails and text messages can be masked to look like they are coming from a trusted sender when they are actually from someone else. Play it safe, do not send your personal information such as account numbers, social security numbers, passwords etc. via email or texting.
- 4. Don't download that file!** Opening files attached to emails can be dangerous especially when they are from someone you don't know as they can allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a good antivirus program on your computer that is up-to-date.
- 5. Links aren't always what they seem.** Never log in from a link that is embedded in an email message. Criminals can use fake email addresses and make fake web pages that mimic the page you would expect. To avoid falling into their trap, type in the URL address directly and then log in.
- 6. Web sites aren't always what they seem.** Be aware that if you navigate to a Web site from a link you don't type, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify that the Web page you're visiting matches exactly with the URL that you'd expect.
- 7. Logoff from sites when you are done.** When you are ready to leave a site you have logged into, logoff rather than just closing the page.

8. Monitor account activity. Monitor your account activity regularly either online or by reviewing your monthly statements and report any unauthorized transactions right away.

9. Assess your risk. We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found; particularly for members with business accounts.

Some items to consider when assessing your online banking risk are:

- Who has access to your online business accounts?
- How and where are user names and passwords stored?
- How strong are your passwords and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?
- Do you have dual controls or other checks and balances with respect to access to online banking transactions?
- Do you have strong antivirus protection and firewalls on your personal computer?

What to Expect From Riverbank Federal Credit Union

- We will **NEVER** call, email or otherwise contact you and ask for your online password or other online banking credentials.
- We will **NEVER** contact you and ask for your debit card number or 4-digit PIN. The only exception may be if you submit a new debit card application and forget to provide us with the PIN.
- If you receive a phone call from the Credit Union and you are not sure if the person is really a representative of RFCU, ask for their name and department and inform the representative that you will call them right back.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, the Federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are described in the Account Information Disclosures you received when you opened your account with Riverbank FCU. You can also find them online under the "Important Account Information" link at www.riverbankfcu.com. Ultimately, if you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 860-292-2940.

For additional information go to:

Onguardonline.gov