SAFEGUARDING YOUR INFORMATION

In today's high-tech world, we are able to do things more quickly and conveniently. We can send a letter via email, pay bills electronically, or even shop online. However, this increase in speed and convenience also increases your risks. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At Firestone Federal 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. Please take a moment to read this important information on how to keep yourself safe when conducting business online or by mobile banking.

HOW TO KEEP YOURSELF SAFE IN CYBERSPACE

An important part of online safety is knowledge. The more you know, the safer you will be. While you may think of cyberspace in terms of regular internet access, many mobile devices (iPhones, iPads, etc.) may be just as powerful as regular computers and often allow you to conduct the same transactions. Here are some tips on how to stay safe in cyberspace:

1. Set strong passwords. A strong password is a combination of upper and lower case letters and numbers and symbols as well as one that is not easily guessed. Change your password frequently. Do not write it down or share it with others. And in your mobile device, do not store passwords.

2. Password protect your mobile device. A device password can help prevent unauthorized access to your information if your mobile device is lost or stolen.

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 number, or passwords via email or text. Do not respond to text messages requesting personal information. Be sure to delete frequently any text messages between you and a financial institution.

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. As an additional measure of protection, make sure you have a good antivirus program on your computer that is up to date. On your mobile device, download applications only from trusted sources.

5. For mobile devices using the Android operating system. Do not enable Android's "install from unknown sources" feature.

6. Do not modify your mobile device. Modifying your mobile device may disable important security features.

7. 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, directly type in the URL address and then log in.

8. Websites aren't always what they seem. Be aware that if you navigate to a website directly through a link, you may end up at a site that looks like the correct one, when in fact it is not. Take time to verify that the web page you are visiting matches exactly with the URL that you would expect.

9. Log off from sites when you are finished. When you are ready to leave a site you have logged into, log off rather than just closing the page.

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

11. Secure your mobile device. Keep your mobile device with you or secure it when not in use. And if your mobile device is lost or stolen, notify your carrier and financial institution(s) so that it can be deactivated.

12. Reset your mobile phone to original factory settings and erase personal information when discarding or selling. It is a good idea to reset your mobile phone and erase personal information before selling, recycling, or donating the device. It is important that you do not leave personal information on the phone and have it accessible to whoever subsequently owns it.

13. Assess your risk. We recommend periodically assessing your online banking risk and putting into place increased security controls where weaknesses are found. This is especially important for members with business accounts. The following are some items to consider when assessing your online banking risk:

- Who has access to your online accounts?
- How and where are user names and passwords stored?
- How strong are your passwords and how often are they changed? If you have a business account, 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?

SUSPICIOUS ACTIVITY - If you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 234-352-1100 or 888-740-8351

RIGHTS AND RESPONSIBILITIES With respect to 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 FFCU. Your periodic account statement also contains disclosures concerning your rights and responsibilities. Contact us immediately if you think your statement is wrong or if you need more information about a transfer listed on this statement.

Consumer accounts have certain Electronic Funds rights under the law. We must hear from you no later than 60 days after the FIRST statement on which the Consumer Electronic Funds problem or error appeared. (1) Tell us your name and account number.(2) Describe the error or the transfer about which you are unsure. Explain as clearly as you can why you believe there is an error or why you need more information. (3) Tell us the date and dollar amount of the suspected error. We will investigate your complaint and will correct any error promptly. If we take more than 10 business days to do this, we will credit your account for the amount you think is in error so that you will have use of the money during the time it takes us to complete our investigation.