MEMBER EDUCATION

SEATTLE
CREDIT UNION

SECURITY AWARENESS AND FRAUD PREVENTION

Seattle Metropolitan Credit Union DBA Seattle Credit Union (hereafter “Seattle Credit Union”) is dedicated to protecting your private information and making sure that you know the best ways to keep your money and your data as safe as possible. Being aware of potential risks can be a powerful first step in reducing your exposure to fraud and identity theft. For more information about these and other current scams, visit https://www.consumer.ftc.gov/scam-alerts and https://www.identitytheft.gov.

SECURITY AWARENESS

1. SYSTEM ACCESS INFORMATION

- Seattle Credit Union will never call, email, or otherwise contact you to request your access ID, password, or other log-in credentials for the online services we offer. If you receive such a request, do not provide any information. Contact Seattle Credit Union to report the incident.

2. PASSWORD SECURITY TIPS

- Do not share your username or password with anyone. Keep them in a secure location. Only you should have access.
- Create a unique username and password for each website, and do not use the same identifying information on multiple sites.
- Create strong username and password and include upper case letter(s), lower case letter(s), number(s), and special character(s), like !@#$%^&*.
- Change your password on a regular basis.

3. REPORTING SUSPICIOUS ACTIVITY

- If you see suspicious activity on your account(s) or have received a suspicious call, email, letter, or other similar activity relating to your accounts, report this to Seattle Credit Union immediately.
- Consumer Protection and Regulation E: The regulation provides rules for error resolution and unauthorized transactions for electronic fund transfers, which includes most transactions processed online. In addition, it establishes limits to your financial liability for unauthorized electronic fund transfers. These limits, however, are directly related to the timeliness of your detection and reporting of issues to Seattle Credit Union. We encourage you to immediately review periodic account statements and to regularly monitor your account activity online. The disclosure provided to you at the time of account opening provides detailed information. We will provide to you, upon request, a free printed copy of this disclosure.

4. ONLINE ACCESS RISK

- The security tips and links to websites in this document provide important information to help you understand online transaction risk and options to help you control these risks. It is important to be informed. When it comes to internet fraud, account takeover, and identity theft, these steps will help prevent exposure to additional risks.

5. WEBSITE SECURITY TIPS

- Monitor your account activity. View account activity online on a regular basis. Review periodic account statements and reconcile them to your personal records. Report any suspicious activity to Seattle Credit Union immediately.
- When logging off from a website, do not just close the page or "X" out. You need to “Log Out” or “Log Off”.
- Secure websites have a web address that begins with “https" rather than “http”. If this is lacking, the site is not secure. Do not log in or conduct business on the site.
- If a website displays a security monitor, verify it has the current date. If it does not, do not use the site; it may be a spoofed or hijacked.
- When completing financial transactions, verify encryption and other security methods are in place protecting your account and personal information.

6. COMPUTER AND NETWORK SECURITY TIPS

- Use quality security monitoring software on your PC that includes anti-virus, anti-malware, and firewall functions.
- Use your PC's security features, such as individual Log-In accounts.
- Keep your PC's operating system security up-to-date by applying patches and updates.
- Password-protect your computer network (physical or wireless).
- Use web resources to learn more and do more to protect yourself online.

7. HELPFUL LINKS

- Two user-friendly sites for users of all ages and interests:

  http://onguardonline.gov

  http://www.staysafeonline.com

- Consumer alerts and online security tips on the FTC website:

  http://www.ftc.gov/bcp/menus/consumer/data/privacy.shtm

8. RECENT SCAMS AND HOW TO REPORT SCAMS

- Go to the IC3 website, a partnership of the FBI, the National White Collar Crime Center, and the Bureau of Justice: http://www.ic3.gov.

9. SCAMS, FRAUDS, AND TIPS TO AVOID BEING A VICTIM

- Go to the FBI website at: http://www.fbi.gov/scams-safety.
- Learn more about scams and prevention: http://www.fakechecks.org/index.html.

10. INFORMATION FOR BUSINESS USERS OF ONLINE SERVICES

Financial regulators have noticed that business transactions, because of their frequency and dollar value, are inherently riskier than consumer transactions. The fraud risk is increasing, e.g., rise of online account takeovers and unauthorized online fund transfers related to business accounts. Small to medium sized businesses have been primary targets as cyber criminals have recognized that the security controls they have in place are not as robust as that of larger businesses.

Here are some of the financial regulators' suggestions to enhance controls for businesses:

- Business members should perform a periodic risk assessment and an evaluation of the effectiveness of the controls they have in place to minimize the risks of online transaction processing.
- The password, website, computer and network tips above provide a starting point for this process, and the web resource links provide additional detailed information.
- The FTC Business Center has a great deal of information for businesses at http://business.ftc.gov/privacy-and-security/data-security.
- Business members should understand the security features of the software and websites they utilize and take advantage of these features. Segregation of duties—the process of separating duties, so no one person can perform all steps of a transaction—is an example of a very important security feature.
- Layered security options that may be available to business members doing online transactions include transaction thresholds, out-of-band verification (such as telephone or email verifications), fraud detection and monitoring systems, and IP reputation–based services.

IMPORTANT FRAUD PREVENTION TIPS

1. ALWAYS REMEMBER:
   - If it sounds too good to be true, it probably is.
   - Never provide your online banking credentials to anyone.
   - Trust your gut feelings – especially when you have a bad feeling about an offer or a company.
   - If you are ever asked to deposit a check or money order, then wire funds – this is a scam.

2. ATM SECURITY TIPS:
   ATMs can be subject to fraud, vandalism, and burglary. They can also be the scene of robberies. Consider the following tips when using an ATM:

   - Use a familiar ATM when possible. If you are not near one, choose a well-lit, well-placed ATM where you feel comfortable. If possible, use a drive up ATM especially if you're alone at night. Keep your car doors locked and your windows up, except for the driver's window when using the machine.
   - Scan the entire ATM area before using the machine. Avoid using the ATM if anyone is loitering or if it looks too isolated or unsafe. Trust your instincts.
   - When using a walk-up ATM, avoid opening your purse, bag or wallet. Have your card ready in your hand before you approach the machine.
   - Observe if anything looks unusual or suspicious about the ATM indicating it might have been altered. If the ATM appears to have its card slot or keypad altered, do not use it. Check for unusual instructions on the display screen or for suspicious blank screens. If you suspect that the ATM has been tampered with, proceed to another ATM and inform Seattle Credit Union or the ATM owner.
   - Avoid an ATM which has a message or a sign attached to it indicating that the screen directions have been changed, especially if the message is posted over the card reader. Seattle Credit Union and other financial institutions will never post messages directing you to use an ATM that has been altered.

3. ATM SKIMMING SECURITY TIPS:
   Skimming is a method of obtaining personal data from ATM, debit, or credit cards while they are used at an ATM machine or a merchant location. People can alter equipment on legitimate ATMs in an effort to steal both the magnetic stripe data from the cards being used and the PINs that are assigned to those cards.

   Equipment is installed on the front of the original ATM card slot. The false slot holds an additional card reader called a "skimmer." The skimmer captures and copies the card information.

   Then a camera that reads the card PIN is housed in an innocent looking pamphlet holder. The camera inside pamphlet holder is angled to view monitor and keypad.

   More recent technology allows the culprit to remain nearby receiving the information wirelessly from equipment they installed on the ATM. The thieves can then copy the cards and use the PIN numbers to withdraw money from many accounts in a very short time directly from an ATM.

   Please note: The examples refer to ATMs, but similar devices may also be placed on card readers at gas station pumps.

   What can you do to protect yourself?
   Be vigilant and inspect the ATM before using it. Skimming devices that are placed on or near the ATM's actual card reader are often difficult to detect, but if anything about the card reader or PIN pad looks different, unusual or seems loose to the touch, don't use it. If possible, report this to Seattle Credit Union or the owner of the ATM as soon as possible.

   What if a skimming device is found on an Seattle Credit Union ATM?
   If you suspect a skimming device has been placed on a Seattle Credit Union ATM, do not use it or try to remove the device. Speak to branch personnel as quickly as possible or call our Contact Center at 206.398.5500.

4. PHISHING SECURITY TIPS:

Phishing is a technique that uses fake emails or fraudulent websites to gain personal information for purposes of identity theft. The fraudulent email messages and/or websites are designed to trick recipients into divulging personal financial data such as credit card numbers, online banking login credentials, social security numbers, etc.

Sometimes, phishers will create a fake website that looks legitimate and attach a link to the fake website in an email. Unsuspecting recipients that click on this link will find that the website that opens up that resembles the correct website. However, the computer user does not know that they have been redirected to a fake website which can be designed to collect personal information.

- Be suspicious of any email requiring an urgent response from you and seems alarming or exciting. Phishers will send emails requiring your immediate attention or to "verify their records." They usually ask for information such as usernames, passwords, account numbers, social security numbers, etc. Emails from phishers are generally not personalized and may appear to be sent in mass distribution.
- Do not click on links sent in an email that is asking for information. Emails suggesting to "click here" in order to enter personal information may end up redirecting you to a fake site that could be collecting your data for malicious use. If you are unsure of the legitimacy of an Seattle Credit Union email, contact us at 206.398.5500.
- Avoid filling out forms asking for confidential or financial information unless you are dealing with a reputable site that you can verify as authentic. If you enter any information, make sure that it is done over a secure link (SSL). This can be verified by checking the "lock" icon in your browser window or displaying https:// in the address bar. (https:// - the "s" represents secure).

5. FRAUD SCAMS

Don’t fall for these scams, explained in detail at http://www.seattlecu.com/fraud-protection.

- Lottery/Sweepstakes Scam
- iTunes Card Scams
- Craigslist/Overpayment Offer Scam
- Mystery Shopper Scam
- Car Wrap Scam
- Romance Scam
- Unexpected Inheritance Scam
- Credit Card Telephone Scam