Sovita℠ CREDIT UNION

4411 Calkins Road • PO Box 320830
Flint, MI 48532-0015 • 810.720.8300

Internet Fraud Warning

In an effort to educate our members, Sovita Credit Union is providing information about potential threats to your personal identification and account information. By obtaining the facts about online and email fraud, you will be better able to protect your private information.

Sovita Credit Union Representatives will never ask you to provide account or other personal identification via email. Be extremely suspicious of any email asking you to log in to the Sovita Credit Union Web site if it does not link to a legitimate Sovita Credit Union site located at the following addresses:

www.sovitacu.org or www.sovitacu.com

In addition, never provide any personal identification information if the request is coming from an unsolicited email or telephone call. Examples of personal identification information are as follows:

- Account Numbers
- Credit Card Numbers, CVV codes, and card expiration dates
- Passwords, Personal Identification Numbers (PINs), and Personal Identification Codes (PICs) Social Security Number
- Mother's Maiden Name
- Other Private Information

If you receive an email or pop-up message asking for account information and claiming to be from Sovita Credit Union, please contact us immediately at **(800) 369-2786, (810) 720-8300 or (810) 664-5351.**

Phishing

Phishing is a form of identity theft. It is when thieves send an email or pop-up message and ask you to provide your personal information.

The thieves often pose as a:

- Financial institution
- Credit card company
- Online merchant
- Utility or other biller
- Internet service provider
- Government agency
- Prospective employer

Here's how phishing works: Consumers receive an email or pop-up message, which appears to be from a trusted organization with which they do business. The email typically includes false appeals such as problems with an account or billing errors, and asks the consumer to confirm personal information. Different approaches include things such as "We're updating our records", "We've identified fraudulent activity on your account", or "Valuable account and personal information was lost due to a computer glitch". To encourage people to act immediately, the email usually threatens that the account could be closed or canceled.

Most emails ask recipients to follow an embedded link that takes them to an exact replica of the victim company's Web site. Graphics on the counterfeit site are so convincing that even experts often have difficulty distinguishing the fake site from the authentic one.

Despite the convincing appeals, members should never respond to unsolicited emails that direct them to divulge personal identifying information. Reputable organizations that members legitimately do business with generally do not request account numbers or passwords unless the member initiates the transaction.

Security precautions for Internet users:

If you encounter an unsolicited email that asks you, either directly or through a Web site, for personal financial or identity information (such as social security number, passwords, account numbers or other identifying information) **DO NOT RESPOND.**

Most companies require you to log in to a secure site. Look for the “padlock” icon at the bottom of your browser and “https” in front of the Web site address, which indicates the information will be transmitted over a secured server.

Take note of the header address on the Web site. Most legitimate sites will have a relatively short internet address that usually depicts the business name followed by .com, .net or. org. Fake sites are more likely to have an excessively long string of characters in the header with a legitimate business name somewhere in the string, or possibly not at all.

If you have any doubts about an email or Web site, contact the legitimate company using an address or telephone number that you know to be genuine. Make a copy of the questionable Web site’s URL address, send it to the legitimate business and ask if the address is legitimate.

Do not share your passwords, PINs (Personal Identification Numbers) or PICs (Personal Identification Codes) with anyone.

Do not write your passwords, PINs (Personal Identification Numbers) or PICs (Personal Identification Codes) where others may easily access your information.

Change your passwords on a regular basis. When creating your passwords, do not use information that could easily be linked to you (i.e. phone number, your date of birth, address numbers, etc.). Choose a password that contains ten or more characters consisting of characters from at least three of the following four groups:

- Uppercase letters (A through Z)
- Lowercase letters (a through z)
- Numbers (0 through 9)
- Non-alphanumeric (special) characters (!, @, #, $, &, etc.)

Cybersecurity Tips:

- Make sure a site is a secure (HTTPS) site before entering personal or private information.
- Log-off any site or application you logged into, don’t just close your browser.
- Install an anti-virus package and keep it up-to-date.
- Keep software, programs, applications, and hardware up-to-date.
- Use secure Wi-Fi connections when accessing sensitive information.
- Avoid using public Wi-Fi networks or computers to access your financial accounts.
- Regularly monitor your accounts and notify us immediately of any suspicious activity or concerns. Set up transaction alerts to notify you of account activity such as when your account balance is below a certain amount or when certain transactions post.

Please report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft or by calling 1-877-IDTHEFT.