Sovita℠ CREDIT UNION

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

Sovita Credit Union Web Site Use Rules and Internet Privacy Statement

General Privacy Statement

In keeping with our long-standing commitment to provide our members with the highest quality financial products and services, the Sovita Credit Union has developed and maintains this Web site. We have always placed a high priority on maintaining the confidentiality and security of our members' personal and financial information. Therefore, we have taken prudent and necessary steps to assure that this Web site is secure and information transmitted is confidential.

This document sets the rules for the use of our Web site, explains the types of information we may obtain from visitors and the security measures we use to protect the privacy of our records and the personal and financial information of our members.

Laws and Regulations

Sovita Credit Union controls and maintains this Web site from the United States of America and makes no representation that materials are appropriate or available for use in other locations. User access to and use of this Web site is subject to all applicable international, federal, state, and local laws and regulations. Users of this Web site agree to submit to the laws of the State of Michigan and applicable federal law without regard to conflict of laws principles.

Information Collection and Use

When you browse the Web site and have not registered for any online service from the credit union, you browse anonymously. Personal information—such as your name, address, phone number or e-mail address—is not collected as you browse. We do, however, use "cookies" to inform us how and when pages on our site are visited and by how many people. We use this data to help us determine how many visitors use different parts of our Web site so that we may focus on and improve our Web site to make it easier to use and more helpful for our members and potential members. A cookie cannot retrieve any information from your hard drive, pass on computer viruses, or capture your e-mail address. We do use a cookie to enable our server to recognize you as an authorized registered user of our online services.

We limit the collection of information about our members to what we need to know to administer their accounts, to provide member services, to offer new products and services, enhance this Web site or other marketing materials, and to fulfill any legal or regulatory requirements. In accordance with federal laws and regulations we provide our members with an initial and annual privacy disclosure that informs our members about the general uses of information we collect about them and the security we employ to maintain the confidentiality of their information.

(Click here to view Sovita Credit Union Privacy Disclosure)

Employee Access to Information

We strictly limit access to personal, financial or other information of our members and Web site visitors to credit union officials with a specific business purpose for knowing such information. All credit union officials are aware of and required to follow our established privacy policies and procedures.

Site Content

Although we try to provide accurate and timely information on our Web site, the content on this Web site may not be accurate, complete or current and may include technical inaccuracies or typographical errors. From time to time changes may be made to Web site content without notice. We may change the products, services, and any other information described on the Web site at any time. The information published on the non-secured areas of this Web site is for informational purposes only and as a convenience to visitors. You should verify all information before relying on it and decisions based upon information contained in our Web site are your sole responsibility. If you need more specific details or information about any information contained in our Web site, you should contact us directly.

The products and services referred to on this Web site are offered to our members by Sovita Credit Union or a valued service partner. The products and services and the applicable terms and conditions may change at any time. The availability of these products and services are subject to our field of membership limitations.

(Click here to find out if you are eligible to join)

All of the information on this Web site including all images is proprietary material of Sovita Credit Union, unless otherwise indicated. You may not copy, download, republish, distribute, or reproduce any of the information contained on this site without our express prior consent, unless otherwise indicated.

Access to Password Protected / Secured Areas

This Web site contains areas that are restricted to use only by individuals that have been authorized to access these areas via a password or other user identification code. We utilize appropriate security measures to authenticate the user's identification, insure confidentiality of credit union and member records, protect against any anticipated threats or hazards to the security and integrity of such records, and to protect against any unauthorized access to our use of such records. We regularly test our systems and procedures to assure that our security measures meet our high standards. Any unauthorized individual attempting to access any secured areas of this Web site may be subject to prosecution.

E-mail

Sovita Credit Union welcomes feedback from visitors to this Web site, and you may do so by sending us an e-mail to memberservices@sovitacu.org. If you do choose to contact us via e-mail, please keep in mind that your e-mail address and any other information your e-mail header shows about you such as your name, organization, and e-mail address will be revealed to us. We promise that we will only use your e-mail information for the purpose of responding to your comments or questions. Your information will not be sold or shared with others outside of the credit union, unless we are compelled to do so by law.

Please be very careful when communicating via e-mail as it is not necessarily secured against interception, and we cannot guarantee its confidentiality. We recommend that you not send any private or confidential information to us via e-mail. If you choose to send any such information to us via e-mail we assume no responsibility and you accept all of the risk that it may be intercepted by an unauthorized third party.

Links

We prohibit caching, unauthorized hypertext links to this Web site and the framing of any content available through this Web site. We reserve the right to disable any unauthorized links or frames at any time

This Web site contains links to other Web sites that we believe are of interest and value to our members and visitors. Users should be aware that these Web sites might contain their own rules and regulations, confidentiality provisions, transmission of personal data provisions, and other provisions that differ from the provisions provided on this Web site. Links to another Web site do not constitute our approval or endorsement of that Web site or any products, services, or advertisements on that Web site. Further, we are not responsible for your use of a linked Web site and we expressly disclaim any and all liability related to the use of a linked Web site.

Children

We do not use this Web site to knowingly solicit or collect data or any other information from or market to children under the age of thirteen.

Changes to These Rules

We reserve the right to revise these Rules at any time and users are deemed to be apprised of and bound by any changes to these Rules.

Violations of These Rules

We reserve the right to seek all remedies available at law and equity for violations of these Rules, including the right to block access from a particular Internet address to this Web site.

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.