Gerber Federal Credit Union is committed to ensuring the highest standard of security for our Members. Our online security controls include multi-factor authentication, dual controls for business and operational processes, and multiple redundant layers of security software and hardware. You also play an important role in ensuring that you are protected when you use the Internet. To help you stay safe on the Internet, we recommend the following security tips and best practices.

SECURITY TIPS AND BEST PRACTICES FOR THE INTERNET:

Protect your password

Passwords are one of your first lines of defense. Make your passwords difficult for hackers to guess. An ideal password contains a minimum of eight characters and is a combination of letters (upper and lower case), numbers, punctuation and special characters. Avoid easily guessed combinations like addresses and birthdates. It's a good idea to change your passwords every three months or so and use a different password for each of your accounts. NEVER reply to any emails asking for your password or other sensitive information.

Enhance your computer security

Install anti-virus, anti-spyware and other Internet security software on your PC and keep it up-to-date. You can even schedule updates to run automatically. Make sure the computer you are using has the latest security patches and take advantage of your PC's security features. If you have a wireless network at home, make sure to take the necessary steps to make it secure – such as not broadcasting your network name, requiring a password to connect and changing the default password on your wireless router. Wireless networks in public areas like airports, hotels and restaurants may have reduced security so it's easier for individuals to access and use these wireless networks. Public wireless networks should NEVER be considered secure. You may decide that accessing your online accounts through a public wireless connection isn't worth the security risk.

Be careful when opening email

If you get an email from someone you don't recognize, or if the subject line or the purpose seems questionable – don't open it. Instead, delete the email and any attachments. Don't respond to emails requesting personal information. More often than not, these are phishing emails trying to persuade you to give up your personal information. Legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as email. If you have a reason to believe that your financial institution actually does need personal information from you, pick up the phone and call the company yourself. Email attachments are the easiest method for a hacker to install a computer virus on your machine. It's always a good idea to question the sender of the attachment and know what you are opening. The same goes for an embedded link in the email that you are instructed to click on. Clicking on the provided link and entering confidential information on a fraudulent site could result in your information being compromised or stolen.

Be selective about what you download

When you download a program or file from an unknown source, you risk loading malicious software programs onto your computer or mobile device. Be selective about what you download and update and run antivirus scans regularly.

Log out completely

Closing your browser or typing in a new web address when you're finished using your online account may not be enough to prevent others from gaining access to your account information. Instead, log-out to terminate your online session. Your web browser may offer to remember frequently used passwords and credit card numbers. Although it may make online shopping or banking a little easier, you should decline the offer and enter your username and password manually.

ADDITONAL SECURITY TIPS FOR SMARTPHONES AND TABLETS

Password-protect your mobile device

Your mobile device should be protected with a strong password. Never use the notepad on your phone to keep track of your financial passwords. Don't choose automatic login options, and set your device to auto-lock after a few minutes.

Be careful about downloading apps

Only download apps from a trusted source. App stores have different standards for the apps they will offer to the public. Also, do research on the app itself. Look for apps that have a high number of reviews and read them. Take time to read the app's privacy policy. Check to see if the app needs access to and will report your position via GPS, and whether it will expose your private and personal information to other users or any potential buyer of that data. If you download an app and your device starts preforming differently (for example, responding slowly to commands or draining its battery faster), this could be a sign that malicious code is present on the device. Update all apps when notified.

Do not use public Wi-Fi when preforming financial transactions

Most mobile devices can use both wireless Internet and a mobile provider's 3G or 4G network. Use only 3G or 4G networks for any secure transactions.

Disable Bluetooth settings on your mobile device whenever it is not in use

If Bluetooth is left on, someone could potentially pair to your device and obtain information or take over your device.

Communicate carefully with your financial institution

Understand that your financial institution will never send emails or texts asking for personal information. Don't save messages or emails containing sensitive information.

OTHER SECURTY TIPS AND BEST PRACTICES

***** To avoid identity theft, never release personal or account information to unsolicited e-mails, telephone calls, or text messages. Be cautious of who you give personal or account information to.

***** If you receive an unsolicited email, text or SMS message asking you to verify or provide your account or personal information, do not click on or select any embedded links as they could contain viruses or Trojan horses.

***** If you receive a phone call, email or text message telling you your account will be blocked, locked or closed if you don't respond immediately, do not respond directly to the solicitation or contact. Call or email Customer or Member Service using the contact information your financial institution lists on your account statement or on your debit/credit card to respond. Fraud services may contact you to confirm purchases, but will not ask you for personal information.