

Safeguarding Your Information

In today's high tech world, we are able to do things more quickly and conveniently whether it is to send a letter via email, pay bills or even shop online. With this increase in speed and convenience also comes an increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public.

At Team One 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 and we would like to help you in this endeavor. Please take a moment to read this important information on how to keep your information safe when conducting business online.



If you suspect or notice any suspicious account activity or experience any security-related events with Team One's Online Banking, you should immediately contact us at the following:

Team One Credit Union
M - Fri 9:00 am - 5:00 pm
Excluding Holidays

You can also stop by any Team One branch to report suspicious account activity or discuss any security-related events within Team One's Online Banking.

Main Office-Saginaw
Downtown
520 Hayden St.
P.O. Box 1260
Saginaw, MI 48607
989-754-6575

Saginaw Township
4075 McCarty Rd.
Saginaw, MI 48603
989-799-9326

Thomas Township
8450 Gratiot Rd.
Saginaw, MI 48609
989-781-5044

Bad Axe
499 Brick St.
P.O. Box 146
Bad Axe, MI 48413
989-269-9557

Bay City
401 E Midland St.
Bay City, MI 48706
989-671-0077

Caro
1130 Cleaver Rd.
P.O. Box 64
Caro, MI 48723
989-673-2042

Sandusky
625 S. Sandusky Rd.
P.O. Box 328
Sandusky, MI 48471
810-648-3900

Owosso
1259 East Main St.
Owosso, MI 48867
989-723-2243

Traverse City
Regional Loan Center
415 Cass St., 2B
Traverse City, MI
49684
231-346-6490

Alpena
Regional Loan Center
122 W. Chisholm St.
Alpena, MI 49707
(989) 419-2020



Authentication in an Internet Banking Environment



How to Keep Your Information Safe Online

An important part of online safety is knowledge. The more you know, the safer your information will be. Here are some great tips on how to keep your information safe online:

1. Set good passwords.

A good password is a combination of upper and lower case letters and numbers and one that is not easily guessed. Change your password frequently. Don't write it down or share it with others.

2. 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 untrustworthy. Play it safe; don't send your personal information such as account numbers, social security numbers, passwords, etc., via email or text messages.

3. Be careful with that attachment.

Opening files attached to emails can be dangerous especially when they are from someone you don't know as they may contain harmful malware or viruses. Make sure you have a good antivirus program on your computer that is up-to-date.

4. Links aren't always what they seem.

Be careful when logging 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 you can type in the URL address into the browser.

5. Websites aren't always what they seem.

Be aware that if you navigate to a website from a link you didn't type, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify that the web page you're visiting matches exactly with the URL that you'd expect.

6. Logoff from sites when you are done.

When you are ready to leave a site you have logged in to, logoff rather than just closing the page.

7. Monitor account activity.

Monitor your account activity regularly either online or by reviewing your monthly statements. Report any unauthorized transactions right away.

8. Assess your own risks.

We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found; particularly for members with business accounts.

Some items to consider when assessing your online banking risk are:

- Who has access to your online business accounts?
- How and where are usernames and passwords stored?
- How strong are your passwords and how often are they changed? (For businesses, 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 for access to online banking transactions?

What to Expect from Team One

- Team One will NEVER call, email or otherwise contact you for your username, passwords or other online banking credentials.
- Team One will NEVER contact you for your credit or debit card number, PIN, or 3-digit CVC (security) code. Please see below for more information about how our credit and debit card provider approaches customer service calls.

Credit & Debit Cards

Our card provider may contact you on behalf of Team One Credit Union to verify unusual credit or debit card transactions. They identify themselves as from the Fraud Center. They will NEVER ask for your card number, expiration date, CVC (security) code or Team One account information.

If you are uncomfortable with the call, please hang up and contact Team One Credit Union at 1-888-288-3261.

Protection Under Regulation E

Regulation E, better known as the Electronic Fund Transfer Act (EFTA), outlines the rights, liabilities, and responsibilities of consumers that use electronic services covered under the EFTA and financial institutions that offer services covered under the EFTA.

Examples of EFTA covered electronic services offered by Team One

- ATM (Automated Teller Machine)
- ACH (Automated Clearing House)
- Debit Card Transactions (point-of-sale)

Examples of services not covered by EFTA

- Share Drafts (checks)
- Wire Transfers
- Internal transfers between members' accounts initiated through a members' online banking account.
- Internal transfer requests made via telephone conversation or in person with a Team One employee.
- Internal transfers to a loan done through online banking, telephone conversation, or in person. Also includes internal recurring transfers that members have requested.

The above are just examples and are not an exhausted list of EFTA covered and uncovered services.

For more information on your rights, responsibilities, and liabilities under EFTA, please review Team One's Membership and Account Agreement that was provided to you at account opening.

You can also obtain a copy of the agreement of your account from the Team One website at www.teamonecu.org.

