

CREATING STRONG PASSWORDS

- ☑ Change passwords regularly.
- ☑ Don't use easy-to-guess information such as your name, date of birth, phone number, address, etc.
- ☑ Don't include your password in any file, including a word processing document, web page, or email message.
- ☑ Avoid using the same password on different systems. If an unauthorized user gets your password, they could gain access to multiple systems.
- ☑ Where possible, use a combination of letters, numbers and characters in your password. Those types of passwords are more difficult to guess. A good rule to follow is not to use any word found in a dictionary. Also, don't use repeated or easily guessed numeric values (such as 1111 or 1234).

ADDITIONAL RESOURCES

Information about malware, phishing and identity theft can be found on our Digital Safety page on our website at www.UnitedOne.org along with links to these resources:

- www.staysafeonline.org
- www.ftc.gov (Federal Trade Commission)
- www.usa.gov
- www.annualcreditreport.com



Click on this icon on our website to view our SmartOne Financial Wellness blog, which contains consumer protection articles to help you manage your account.

YOUR RIGHTS & RESPONSIBILITIES

When it comes to online banking and electronic funds transfers, the Federal government outlines your rights and responsibilities in the Electronic Fund Transfer Act (EFTA), often referred to as Reg. E. This information was provided to you when you opened your account. You can request a copy of it from us anytime.

AFTER-HOURS CARD ASSISTANCE

For after-hours assistance regarding a compromised debit or credit card, please do the following:

For Your **Debit Card**, call **920-684-0361** or **920-451-8222** and then select 6 for the Debit Card Menu.

For Your **Credit Card**, call **800-558-3424**. Your call will be answered by "Cardmember Service."



UnitedOne Credit Union is open to everyone living or working in Manitowoc, Sheboygan, Kewaunee and Door Counties.



UnitedOne.org
mail@UnitedOne.org



Manitowoc 920-684-0361
1117 S. 10th St.
Walmart SuperCenter

Sheboygan 920-451-8222
3509 Washington Ave.
2122 Superior Ave.
The Encore, 733 N. 8th St.



Insured by NCUA
08/22

We're here because you're here!

STAYING SAFE IN A DIGITAL WORLD





TAKING MEASURES TO PROTECT YOUR FINANCIAL STRENGTH, TOGETHER

Here at UnitedOne Credit Union, taking measures to keep your finances safe and secure is an ongoing mission.

In today's digital world where more people are transacting business electronically more than ever, it's unfortunate individuals are working hard to find new scams to target unsuspecting consumers. One of the best ways to avoid becoming a victim is by becoming an educated consumer. We're here to help you with the following information and additional resources listed in this brochure.

TIPS FOR KEEPING YOUR ACCOUNT SAFE

- **Monitor your account activity regularly** by using Digital Banking or Touch Tone Teller, even if you don't have transactions often. The sooner you identify any potential problems, the sooner we'll be able to help you fix them.
- **Consider setting up free Alerts** within Digital Banking, Bill Payer and your credit card. These Alerts notify you of activity relating to many different types of transactions. You choose the specific alerts you want.
- **Never share PINs, passwords or account numbers** for your debit or credit card, Digital Banking, Touch Tone Teller, etc. Do not write them in any place that can be seen or found by others.
- **Keep your personal information private.** Emails and text messages can be masked to look like they are coming from a trusted source. Do not send your account number, debit or credit card number, Social Security number, passwords, etc. by email or text message, unless you're using a secure email system with which you are familiar.



PROTECTING YOUR DIGITAL ACCOUNTS

- **Log off sites when you're finished**, rather than just closing the page, especially when monetary transactions are involved. It's much safer.
- **Make sure your browser's padlock or key icon by the URL is active when making purchases online.** Also, look for an "s" after the "http" to be sure the website is secure.
- **Use multi-factor logins whenever possible.** This extra layer of security requires not only a password, but confirmation from another device only you possess, like your mobile phone.
- **Use caution about what you post on social media.** Hackers and scammers could use the information you share to learn your passwords and potentially steal your identity, or use it against you in other ways.
- **Be vigilant about your surroundings when entering passwords in public settings.** Avoid conducting financial transactions or using business accounts through public WiFi.
- **Be aware of redirection.** Like many businesses, UnitedOne works with partners who operate websites we either make available for your convenience, or believe you may find helpful. You can get to those sites from our website. Our site has pop-up warnings letting you know when you are being redirected to a site we do not operate. Notify us if you suspect any problem with redirection.
- **Do not download files attached to, or follow hyperlinks in, emails.** This can be very dangerous, especially when they are from someone you do not know. This is how malware and viruses are often downloaded. Go directly to a site that is hyperlinked by entering its URL address into your browser, and take time to verify that the web page you're visiting matches exactly with the URL you'd expect for that site.



COMMUNICATING WITH UnitedONE & OUR SERVICE PARTNERS

If you are ever uncomfortable when communicating with any of our card partners, feel somebody is posing wrongfully as a UnitedOne Credit Union employee, or if you suspect your financial safety has been compromised, please contact us immediately during regular business hours at: 920-684-0361 or 920-451-8222.

Our partners who may contact you for member service surveys or auditing purposes are MemberXP and Leede Research.

- We will never call, email or contact you in any other manner asking for your member ID, account number or online banking passwords.
- We will never contact you asking for your credit or debit card number, PIN, or security code.
- To ensure our employees are helping the correct member they may ask you questions that only you would be able to answer, like where did you use your card last or where does your direct deposit come from. This is for your protection.
- Neither our debit card nor our credit card provider will initiate contact by email regarding a problem with your cards.
- As a UnitedOne debit card holder you get the added protection to have fraud monitoring on your card. Our Visa Fraud Department may notify you if it notices any unusual transactions with your card. They may call or text to question if a transaction was authorized by you. If the answer is no, your card is shut down immediately. Your card may not work properly until confirmation of the transactions in question is received.

