

Safe Online Banking Practices



At Meritus Credit Union, we are committed to ensuring that your account information is safe. It is important that you help protect your computer and account information, too. We recommend that you take precautions to help prevent the compromise of your online banking account.

Online Safety Precautions

- **Set strong passwords**
Create a password that is a combination of upper and lower case letters, numbers, and special characters. Change your password regularly and don't share it with others.
- **Protect your personal information**
Emails and text messages can be masked to look like they are coming from a trusted sender. Do not send your personal information such as account numbers, social security number, passwords, etc. via email or text.
- **Keep your computer healthy**
Use anti-virus software, a firewall and spyware detection software to help keep your computer safe and secure. Opening files attached to emails can be dangerous, especially when they are from someone you don't know, since they can allow harmful viruses.
- **Avoid scams to steal your identity**
Don't click on any links within an email asking you to access your account or to verify PIN numbers, passwords, or other sensitive information. Criminals can use fake

email addresses and suspicious web pages that look legitimate. If you receive an email, immediately contact us to report the incident.

- **Protect your card when shopping online**
Shop at reputable websites. When you go to the payment screen to enter your card number, make sure there is an "s" in the beginning of the web address ("https"). This represents "secure".
- **Logoff from sites when you are done**
When you are ready to leave a website you have logged in to, logoff instead of just closing the page.
- **Monitor your account activity**
Review your account regularly either online or with your financial statements. Report any unauthorized transactions.
- **Assess your risk**
Assess your online banking security controls such as, but not limited to: storage of online banking information (account number, password, PIN, answers to security questions), and the type of antivirus protection you use on your computer.

What to Expect from Meritus Credit Union

- Meritus CU will **NEVER** call, email, text or otherwise contact you and ask for your online banking user name, password or other sensitive information.

- Card fraud detection may contact you on behalf of Meritus CU to verify unusual credit or debit card transactions. They will **NEVER** ask you for your credit or debit card number, PIN, 3-digit security code on the reverse of the card or expiration date.

Learn More About Safe Online Banking

www.ftc.gov
www.idtheft.gov

If You Suspect a Compromise

If you suspect or experience any suspicious activity with your Meritus Credit Union debit/credit card or accounts, please contact us immediately.

Debit Card & Account Fraud

1.866.989.2800

Credit Card Fraud

1.800.600.5249

You can also visit any Meritus CU branch location during normal business hours to report suspicious account activity or discuss any Meritus CU security-related concerns.

R05/22

Smart Financial Solutions.



337.989.2800 | 866.989.2800 | merituscu.net