4 BEST PRACTICES

TO PROTECT YOUR ONLINE BANKING ACCOUNT

The newest scam targeting financial institutions across the county is called "credential stuffing." Here's what you can do to make sure your accounts remain secure.

Credential stuffing is when fraudsters use previously exposed credentials, such as login names and passwords from hacked sites, to automate log-in attempts on new sites with the hope that the users have re-used the same usernames and passwords elsewhere. When these criminals have a legitimate account on the hook, they contact the account owner and use scam techniques to get into the account. They may pose as bank employees or fraud department personnel to obtain the last bit of information they need to break through that final wall of security. The fraud works when the bad guys call their target victim using a spoofed phone number that looks like it's coming from the financial institution.

While you may get a call from someone at the bank to verify transactions, they will NOT ask for your pin, security code or user names/passwords. If this happens, hang up immediately and call the bank at 1.800.453.8700 to report the fraud attempt. We will never call a customer to ask them for their login credentials or a Secure Access Code! Please follow these four best practices to keep accounts safe and secure:

Create a unique login and password for Online Banking accounts

Do not be tempted to reuse a login and password from another account. If you're currently using a login and password you use elsewhere, change it now. And even if you're not and you notice your login and password aren't that creative, do yourself a favor and spend five minutes making a change. Also, resist the urge to save this new information to your browser.

Use complex usernames

Customers who have easy-to-guess usernames may be vulnerable with this scam. You may be using an email address or just your first and last names. This is just too easy for someone to guess. This is the time to let your creativity shine. Make your login name a phrase only you would know, but that's easy enough for you to remember. Refrain from using this new username anywhere else.

Change passwords frequently

Even if you have complicated, hard-to-guess passwords, with all the data breaches going on, your passwords may become vulnerable at some point. Be smart and change them regularly, especially for sites where the loss would be personally and/or financially devastating.

Consider using a password manager

We get it. With so many sites out there, how can anyone remember a fresh login and password every time? A password manager can make it easier. Just remember one login and one password and let the manager be your brain. It's important, however, that if you use a password manager you use a complex username and password, a duo you've not used elsewhere.

Mercantile Bank of Michigan will never ask for your online banking username, secure access code, or passwords over the phone. **If you have been contacted by someone who claims to be from the bank and wants access to your account, please hang up and report the incident to us at 1.800.453.8700.**

Mercantile® Bank of Michigan

EQUAL HOUSING LENDER