HOW SECURE IS eBANKING AT MERCHANTS BANK?

Merchants Bank's security certificates and anti-virus software are up-to-date and will help to protect you. However, Online and Mobile Banking are only as secure as you make it. It is essential that you take an active role in ensuring your eBanking accounts are secure:

- Change your password regularly.
- Make sure your password is complex – include numbers and upper and lower case letters.
- Never share your password or login ID with anyone. Even joint account owners should each have a separate login ID.
- Always log out when you are finished using online banking. Never just shut your computer off or hit the red X in the upper corner.
- Make sure any electronic device you use is safe and has current virus protection.
- Run an anti-virus scan every month and make sure that the browser and operating system you are using are up-to-date with any new patches.
- Make sure your mobile devices are password protected.
- Do not have your devices remember your login ids or passwords. Always re-type them before each session.

WHEN WILL MERCHANTS BANK CONTACT YOU FOR PERSONAL INFORMATION?

Merchants Bank will never initiate a phone call or email asking you to verify your Social Security number or account number. We may, however, contact you in the following, or simliar, situations:

- If mail is returned for incorrect address and we do not have record of receiving an address change request from you.
- If you are in the process of opening an account with us and we need additional information.
- If you have submitted an Online Bill Payment and there is a question on the address or company information.
- If you are enrolled for Online or Mobile Banking and have not used them for a period of time, or your Online Banking account is locked.
- If you are a business and use our Cash Management services; we may contact you.
- If fraud is suspected on your Merchants Bank debit or credit card.

For your security, if you do not know the bank employee calling you, we encourage you to write down the information being requested and call the person back by dialing your local Merchants Bank office at a number you have verified on your own through a public source, such as a phone book, or call a bank employee you do know personally. Protection of your personal information is always our top priority.

Visit our website to sign up to receive security tips and alerts from Merchants Bank.

Merchants Bank

1-800-944-6285 • www.merchantsbank.com

FOLLOW US ON: YouTube

06/2016

Is Your Identity Safe?

PROTECT YOURSELF WITH PRACTICAL TIPS

Merchants Bank

The Bank that Service Built

PROTECT YOURSELF WITH PRACTICAL SECURITY TIPS

Identity theft is when someone uses your personal information without your permission.

Bank or Credit Card Fraud is when an account is opened fraudulently in your name and unauthorized charges are made.

How does Merchants Bank protect me? Merchants Bank uses a combination of safeguards to protect your information including: employee training, encryption of information, and fraud detection programs.

Things You Can Do to Protect Yourself:

1. Always lock your vehicle. If keeping your laptop or phone in your vehicle, power it down. The wireless signal of your device can send a GPS location to potential thieves.
2. Put private information away when others will be in your home, such as cleaning people, repair people, babysitters or others.
3. Don't leave private information on your work desk.
4. Do not keep large balances in checking accounts that have checks or a debit card connected to them. Transfer excess funds to a savings account instead.
5. If you are not going to use checks, do not order any.
6. Do not provide your Social Security number or personal credit information to anyone over the phone or online unless you are the one who initiated the call and are familiar with the business.
7. Protect your bank and credit card Personal Identification Numbers (PINs) and other passwords by changing them frequently, using a combination of letters, numbers and special characters when possible, and not sharing them with others.
8. Keep a list of your credit cards, account numbers, expiration dates and customer service or fraud department telephone numbers in a secure place away from the cards for easy access.
9. Shred all financial statements, credit card offers and any unused cards before recycling them.
10. Never keep your Social Security card in your wallet.
11. Carefully check through your credit card and bank activity regularly and immediately report unusual activity.
12. Be cautious when entering a login ID and PIN for all online account access, especially when on a public network. Make sure you are on a secure website.
13. Never have a website remember your password to log in.
14. Set up text or email alerts from your bank for certain transactions, such as transactions over $500. Alerts are available through the "Manage My Money" function in Merchants Bank Online Banking.
15. Sign up for eStatements to reduce the likelihood of paper statements being stolen.
16. Make sure the virus protection software on your computer is up-to-date.
17. Use the passcode feature on your smart phone and other mobile devices. It will be more difficult for people to access your personal information in the event it is lost or stolen.
18. Social media sites ask for your personal information and make it viewable to the public. Be careful what you post on social media websites and check your privacy settings. Criminals can use information such as birthdays, high schools, colleges, pet names, and email addresses to steal your identity.
19. If a financial situation is presented to you that sounds too good to be true, it probably is. You can't win the lottery if you haven't entered. You don't need to send a payment to claim your lottery winnings.

Visit www.merchantsbank.com for more information.

TRAVELING? NOTIFY THE BANK.

Contact Merchants Bank if you will be using your Merchants Bank debit or credit cards while traveling outside the tri-state area. If we are unaware of your travel and see unusual activity on your cards, we may shut down the usage for your protection.

We suggest traveling with more than one card and keeping cards separate so that if one is lost or stolen and needs to be shut down, you are not left without a card.

PROPERLY DISPOSING OF YOUR MOBILE DEVICE

When you upgrade to a new mobile phone, it's important to delete any personal information – like addresses, phone numbers, passwords, logins and so on – on your current device. Please go to http://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device for more information on how to protect your information. Do not simply depend on the cellular company to clean the phone for you.

For more details on these and other security tips, please visit www.merchantsbank.com. You may also follow us on Facebook for new security alerts or subscribe to our Alerts email list, both found on our website.

CHECK YOUR CREDIT REGULARLY

We recommend you check your credit report annually to make sure your history has been recorded correctly. It also will help you identify any suspicious activity and possible identity theft. Three credit bureaus offer a free annual credit report. You can get one, two, or all three at the same time. We suggest you alternate credit bureaus and check your credit report every four months.

Here Are Three Ways To Request Your Free Annual Credit Report:

1. **Website:** www.annualcreditreport.com
2. **Telephone:** (877) 322-8228
3. **Form to request your credit report:** The form can be printed from www.ftc.gov/credit. Or, contact Merchants Bank, and we can help you get the form.

If you would like your credit score, there is a cost, but the annual reports are free.

Remember, you must make the request. Do not respond to contacts – like pop-up messages, emails or texts – they could be a scam.

Contact Merchants Bank at 800-944-6285 to report suspicious account activity.