Citizens Bank
Security Guidelines

The safety of the money in your accounts and your financial information is very important to us, and that is why we would like to take this opportunity to explain recent threats and attacks that have been carried out at other financial institutions. Hackers are focusing their attention on Internet Banking, but the source that they are attacking is not the financial institution that hosts the website. Instead, they are targeting the customer. They send fraudulent emails that contain malware. This malware harvests personal information including your internet banking username and password which can be used to access your information as well as your bank account. Recent attempts appear to come from NACHA or the Federal Reserve Bank. Be assured that neither entity will contact you via email to notify you of a rejected file or problem with your account. All communication about your account will be performed by us, and we will not contact you via email to notify you of a threat. If you receive an unknown email, it is best to delete it without opening it. If you are unsure about the validity of the email, do not open it. You may contact us, and we will help you through the process. As the financial institution, we cannot protect against this type of attack because the information is being harvested on the user end and not on our end. What we can do is educate you about the attack and methods for reducing the likelihood of your account becoming compromise.

Remember that protecting your account and internet banking passwords depends on you implementing and following strong security procedures. Following the guidelines listed below will reduce the likelihood of your account becoming compromised but cannot guarantee your safety. The goal of any security procedure is make it more difficult for the system to become compromised. The following list is an example of what can be done, but is not considered to be comprehensive. If you are concerned about the security procedures in place or believe your account has been compromised, please contact us at 573-683-3373 or 573-649-5300 or write us at 207 E Commercial St, Charleston MO 63834 or 722 N Martin St, East Prairie MO 63845.

1. Use virus and spyware protection software. Keep the software updated to protect against new threats.

2. Use software or hardware firewalls to protect your computer from hackers.

3. Never use unsecured public wireless systems for banking services.

4. Do not download files, install software or open email attachments from unknown sources.

5. Change passwords often.

6. Do not use the same password for Internet Banking that is used for other internet activities.

7. Do not give your password or other logon information to anyone that you do not want to have access to your accounts. Do not leave or store this information where someone can find it.

8. Use passwords made up of random numbers or letters. Do not use anything that can be guessed easily such as initials, address, name or birthdate.

9. Disable auto complete features on your computer.

10. Log out when leaving the computer unattended.

11. Do not use any computer that does not belong to you.

12. Do not send confidential banking information by regular e-mail.

13. Install any security-related updates that are provided by your computer manufacturer.

14. Contact us immediately when you notice an error or believe your information has been compromised.

15. If you are contacted by someone purporting to be from the Bank but are not familiar with the person or feel uneasy about the questions being asked, please ask for the employee's name and tell them that you will call them back because you would like to verify you are speaking with a Bank employee. Please utilize the number listed above or another known contact number for the Bank.