HOME NATIONAL BANK
Thorntown • Lebanon

Notice to Internet Banking Users

Purpose

When adopting new technology it is important to know its benefits as well as its risks. Although the newness of internet banking has faded, continuing to learn its advantages and having an awareness of the current potential threats is vital. This notice briefly explains what Home National Bank offers through internet banking, identifies some potential risks, and suggests ways to mitigate them.

Internet Banking Under Reg E

The Electronic Fund Transfer Act (Reg E) affords consumers certain, not businesses, protections against errors, theft, and financial institutions. Reg E applies to a myriad of electronic funds transfers; however, for the purpose of this notice, it applies specifically to internet banking. Simply put, an electronic funds transfer (EFT) is an exchange or transfer of money from one account to another via an electronic mode. With internet banking from Home National Bank, it is possible to transfer funds any time day or night, but it is important for consumers to know their rights and responsibilities.

Each account holder has the right to a monthly statement. Any EFT appearing on a statement must contain any of the following applicable information: the transfer amount, the date of transfer, the type of transfer, to or from what account the transfer was made, the location or ID of the terminal (ATMs), the name of the third party to or from which the transfer was made, and any fees associated with the transfer. It is the account holder's responsibility to review each monthly statement for accuracy or any suspicious activity. If the account holder deems any EFT to be an error or unauthorized, the financial institution must be notified within 60 days of the statement. It is then the responsibility of the financial institution to investigate the transaction. If the account holder fails to notify the financial institution within 60 days of the statement, the consumer is liable for any and all monetary loss.

If the EFT is an error, a notice of error will be provided to the account holder and the error will be rectified immediately. If the EFT is considered by the account holder to be unauthorized the financial institution will examine the transaction to determine if it is actually unauthorized. A transaction is unauthorized if it is initiated by a person, other than the account holder, without the authority of the account holder and the account holder did not receive any benefit from the transaction. A transaction is authorized if the account holder gave the person access to the device, unless the account holder notifies the institution that person is no longer authorized. If the device is lost or stolen, the account holder must notify the financial institution within two business days. Once the account holder notifies the financial institution, the liability for the consumer is the lesser of the amount of the unauthorized transaction or $50. If the account holder fails to notify the financial institution within two business days, the liability increases to the lesser of the amount of the unauthorized transaction or $500.

Internet Banking Credentials

It is imperative to understand that Home National Bank does not make unsolicited calls to its customers asking for information regarding internet banking. Never give out passwords, answers to security questions, or any other personal information to a person or company who has not been solicited for assistance with an account.

Commercial Internet Banking

There is a greater risk associated with commercial internet banking accounts. Since there are greater dangers with these accounts it is recommended, not required that commercial internet banking users operate under the following practices:

- Use an anti-malware program as a defense against attacks.
- Monitor the account regularly for anomalies in transaction frequencies and amounts.
- Require dual control for high value and/or anomalous transactions.
- Use layered security to only allow users to access the functions they will need on internet banking.
- Perform, at minimum, an annual risk assessment and controls evaluation.

Mitigating Risk

There are certain steps internet banking users can take to help mitigate the risks associated with internet banking. Home National Bank recommends that:

- Use an anti-malware program as a defense against attacks.
- Monitor the account regularly for anomalies in transaction frequencies and amounts.
- Users change passwords, authentication questions, and security key regularly.
- Passwords are unique to internet banking.
- Authentication questions should not be easily guessed (i.e. Mother's maiden name, zodiac sign, and nickname).
- Consider setting up authentication questions with "incorrect" answers. For example, a customer's favorite sports team may be the Colts; however, for security purposes, the customer may consider setting the answer to "French fries" as this is a completely absurd answer and would not be easily guessed.
- Do not tell public computers to remember any passwords or authentication questions.
- Always log off when finished.

Questions

It is the goal of Home National Bank to answer any questions that customers may have regarding the security, risks, or features of internet banking. Contact Regina Graddy, or any other Home National Bank internet banking specialist, at 765-436-2222 during normal business hours for more information or assistance.