Clarke County State Bank
Electronic Banking
Safety Tips

Clarke County State Bank wants to help protect your personal information. Please read these various methods, some provided by regulation, some offered by the bank and some requiring customer action, of protecting your information.

Regulation E: Electronic Fund Transfers
The law is designed to protect consumers making electronic fund transfers. The term "electronic" fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's account. The Electronic Fund Transfer Act (also known as Regulation E) establishes the basic rights, liabilities and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. When a banking account is opened, customers receive a Regulation E Disclosure, as required by the EFT Act, which contains detailed information related to the regulation.

Unsolicited Customer Contact
Clarke County State Bank will never contact customers on an unsolicited basis to request their security logon credentials such as the combination of the customer's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at 641-342-6581 or email us at ccsb@clarkebank.com to report any activity of this nature.

Clarke County State Bank (CCSB) may contact customers on an unsolicited basis regarding the following types of activity:

- Suspected fraudulent activity on your account;
- Inactive/dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted to your online banking profile.

Securing Your Environment and Protecting Your Identity
Your identity is one of the most valuable things you own. It's important to keep your identity from being stolen by someone who can potentially harm your good name and financial wellbeing. Identity theft occurs when someone uses your name, address, social security number, credit card or financial account numbers, passwords, and other personal information without your knowledge to commit fraud or other crimes. While the words may sound like a foreign language – phishing, pharming, vishing, spyware, dumpster diving – they are the names of various techniques used by thieves to put your identity and finances at risk. These types of attacks grow more frequent and sophisticated every year.

Business customers are encouraged to review your own unique situation and implement security procedures commensurate with your business' level of risk.

You can protect yourself against most forms of identity theft. The first step is education. To make it easier to understand, we have divided identity theft risk into the following sections:

Email Risk:
Phishing is an email scam used to steal your personal information. Email may appear in your inbox claiming to be from your financial institution, credit card company, or another source. It may appear authentic but be careful – any email requesting personal information or to "verify" account information is usually a scam.

- Never respond to any email asking for confidential information, even if it appears urgent.
- Never click on a link from within an email. Instead, type the known website address into your internet browser.
- Do not call any phone number provided in a suspicious email. It could be a fake number.
- Always use anti-virus and anti-spyware software on your computer and keep them up-to-date.

Remember, email is not a secure form of communication. Feel free to use your email but don't use it to send or receive confidential information.

Internet Risk:
There are several types of malware that can infect your computer as you surf the web including viruses, spyware, Trojan horses, and keystroke loggers.

These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal information. While "surfing" the internet, follow these steps to protect your computer from the majority of internet crime:

- Make sure you have anti-virus and anti-spyware software installed on your computer and keep it up-to-date. Run a full system scan at least weekly.
- Keep your computer operating system up-to-date and your firewall turned on.
- Use strong passwords for secure sites. These should include eight or more characters with random numbers, at lease one capital letter, at least one lower-case letter and a special character such as * & # !.
- If you download anything from the internet such as music, movies, or pictures, make sure you do so only from trusted websites.
- Watch for signs of spyware. Frequent popup ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection. Run a full system virus/spyware scan to identify and safely remove spyware.
- Be careful when using public computers to perform any type of personal transactions. Just logging into a website may give away passwords and other private information if spyware or key loggers have been installed on that computer.

We suggest contacting the store where you purchased your computer for specific guidance on software options to help protect your information.

Telephone Risk:

- Never offer personal or account information over the phone without verifying the caller's identity.
- If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.
- Do not call any phone number received in a voice message or email asking for personal information.

Payment Risk:
Payment fraud happens when someone uses information from your checks, credit and debit cards, or any other form of payment without your knowledge to commit fraud or other crimes. Here are some tips to help protect your identity:

- Balance your checkbook and verify all account and credit card statements as soon as they arrive.
- Keep all checks, credit cards and debit cards in a safe place.
- Don't leave outgoing checks or paid bills in your mailbox and report lost or stolen items immediately.
- Don't write personal identification numbers on your credit or debit cards. Don't leave PINs in your wallet.
- Use a paper shredder to securely dispose of any documents containing personal information.
- Make online purchases only from trusted websites. If you have questions about a company you can check them out with the Better Business Bureau.
- Consider paying all your bills electronically.

Clarke County State Bank Contacts
You are protected in a variety of ways when you use Internet Banking or other electronic services; however, it is important to contact CCSB in the event your online login information has been compromised or if you discover that you have lost your debit card. Also, report any unauthorized or unexpected transactions immediately.

If you want to report suspicious activity on your account, you can call us at 641-342-6581. The security of your money and identity is as important to us as it is to you! Thank you for choosing Clarke County State Bank.