



## Email and Website Fraud Awareness

Some customers may receive email messages that appear to be from Community First Bank that request confidential personal information. These email messages are disguised to look like a Community First Bank message, but are not.

Community First Bank does not solicit confidential customer information this way. These messages are fraudulent and they are not from the bank. If you happen to get one, do not respond to it.

If you have already responded to one of these messages, or have logged on to a site that appeared to be Community First Bank's online site after following a link in one of these, please call the bank immediately at 1-618-244-3000.

### Protect Yourself

Con artists and scams are an unpleasant fact of life, and to criminals the Internet is just another way to take advantage of the unsuspecting. While electronic fraud has become a real problem in recent years, a little knowledge is all you need to protect yourself and your identity.

### What You Need to Know

Electronic fraud is just like any other type of fraud, it's a criminal pretending to be someone they're not. In the electronic world, this can mean emails with forged addresses or websites that are designed to resemble legitimate businesses. These false solicitations always have one thing in common, they ask you to provide personal information, often by asking you to "update your account information" by providing social security numbers, credit card numbers, or other information. Once they have this information, it is easy for an experienced criminal to create a false identity for himself, using your name, and your credit.

While the technology behind these crimes is complex, preventing them is easy. Never give out sensitive personal information online unless you're absolutely certain you can trust the site, and never send out sensitive information in an email.

All electronic contact with Community First Bank, where we request sensitive account information, is done either from our SecureMessage contact site or inside the secure message feature of Community First Bank's Online Banking. If you are uncomfortable with transmitting any financial data online you always have the option to contact us by phone or visit your local Community First Bank.

### Avoid Electronic Fraud

Keep these simple rules in mind and you will be better equipped to protect yourself.

- Never send sensitive personal or financial information through email.
- Don't follow links in an email asking for sensitive personal or account information, even if it looks like the source is one you know.
- Ask questions. If you're suspicious, call the company that the email appears to be from and ask if it is legitimate.
- Install anti-virus software on your computer and keep it up-to-date. Anti-virus programs help protect your computer against most viruses, worms and Trojans that can infect your computer. Most anti-virus software companies provide updates from their websites. Some of the most popular programs are: [McAfee VirusScan](#) and [Symantec's Norton AntiVirus](#).
- Download and use a pop-up blocker from a legitimate source. Some pop-up ads could contain viruses or other harmful software that can record your keystrokes or relay information to another source.
- Equip your computer with either a software firewall or a hardware firewall. A firewall will allow you to limit unauthorized access to your computer.
- Keep your computer operating system, Web browser, and security settings up-to-date. Security patches and updates are usually available from the software vendor's websites.
- Scan your computer for spyware regularly. Spyware is a computer program which can be installed on personal computers, usually without your permission, which may collect information about your website activity and send it back to another source.
- Only keep your internet connection active when you are using it.
- Turn off your computer when you are not using it.

·Never share your PIN, account number, or password.

·Do not open email attachments unless you can trust the source.

·Never access sensitive information from Internet cafes, public libraries, etc.

You can read more about electronic fraud or report suspicious email activity at the Federal Trade Commission website [www.consumer.gov](http://www.consumer.gov).