Information you should know when conducting transactions online.

Each year more Americans have their identity stolen. This document provides information you need to protect yourself against internet threats and other forms of online account takeovers and fraudulent electronic funds transfers. We want you to know that:

1) We will never initiate a request by phone or email for sensitive information such as your PIN, username, password, or other electronic banking credential. We will never ask you to verify your account via email.
2) You should safeguard sensitive information such as your account number, username, password, and PIN. Do not share this information with anyone.

Protect yourself from online risks by:

1) Changing passwords regularly and make them complex by mixing lower case letters, upper case letters, and numbers.
2) Not responding to unsolicited email asking for personal information.
3) Remaining at your computer until your online transactions are completed and log out before visiting other internet sites (do not just close the page or "X" out of the system).
4) Reviewing your account activity often. Call us immediately if you notice suspicious activity with your banking accounts.
5) Using firewalls to protect from outside intrusion or hackers.

For more information on securing your online information refer to the Federal Trade Commission at:

http://www.ftc.gov/bcp/edu/microsites/idtheft
or
http://www.onguardonline.gov

We recommend owners of business accounts periodically perform their own risk assessment and controls evaluation. Create a list of risks associated with online banking that your business faces. Examples include:

1) Written passwords left in plain sight;
2) Simple or obvious passwords;
3) The possibility of internal fraud;
4) Delays in terminating online access of former employees; and
5) Lack of dual control to online transaction capabilities.

Controls your business may use to mitigate these risks include:

1) Assign individual users with complex passwords;
2) Conduct employee background checks;
3) Initiate a policy and process to terminate access for former employees;
4) Segregate duties so no one person has too much access or control; and
5) Conduct internal or third party audits of controls.

Notify us immediately if you believe your access information has been stolen or compromised. Review your account activity and statements and promptly report any errors, unauthorized activity, or security related events. Federal regulations provide consumers some protections and limits liability for unauthorized electronic fund transfers. These regulations generally apply to accounts with internet access. They provide specific steps you must take to resolve an error with your account. You must notify us in a timely manner to take advantage of these protections. For more information on these types of protections see the Electronic Funds Transfer disclosure we gave you at account opening. We will also provide you this disclosure upon request. The disclosure is also available on our online banking site. If you become aware of suspicious account activity, you should contact us at:

Community First Bank
(814) 653-8232