Protect Your Computer or Mobile Device

Protecting your computer is an important part of safe online banking. Steps you can take to keep your computer or mobile device secure include:

- Use an appropriate anti-virus & anti-malware software for your device & keep it current
- Turn on computer firewalls
- Turn on operating system patches & updates
- Do NOT click on links in emails from unknown sources
- Enable your device's screen lock
- Turn off Blue Tooth functionality when not in use
- Do not conduct transactions when connected to unsecured WiFi networks
- Only download apps and updates from reputable sources
- When using apps, make sure you have the most recent version that is available
- Do not send sensitive information via SMS text messaging
- Watch closely for security features
- Contact your wireless provider immediately if your mobile device is lost or stolen
- Do not click on links in emails or text messages

Safeguard Your Credentials

Your online banking credentials enable the bank to identify you and provide information online. It is important that you keep this information safe.

- Never write down or share passwords or PINs with anyone
- When creating passwords or PINs do not use something that would be easily guessed - use a combination of letters, numbers & special characters
- Keep tokens in a secure place
- When creating/answering security questions use information that is not publicly available
- Contact the bank if you suspect your credentials have been compromised

Additional Protection Guidelines

- Email - Do not send personal information via email unless it is encrypted.
- Logging Off – when closing out of your account always use the "Log Out" button and close the browser. This ensures that your session is closed and protects your personal information.
- Do not provide personal information over the phone or via email. The bank collects the necessary information at the time you open your account and will not need to call or email to request it. If you have any doubts please contact the bank.
- Close online accounts that are no longer needed because unmonitored accounts can pose risk.

Common Online Threats

Fraudsters attempt to obtain information from unsuspecting consumers through various methods. Keep your eyes open and be suspicious of unsolicited emails or calls requesting information. Some of the most common types of threats are:

- Malware – software designed to damage or take over your computer. This software installs itself without the knowledge of the user. Viruses, Trojans, worms or spyware are examples of malware.

- Phishing – fraudulent emails that appear to be from a trusted source. These emails typically contain a link that will take the user to a bogus website and ask for verification of personal information which will be used to provide unauthorized access to your account.

- Pharming – fraudster reroutes the user to a site other than the users intended site. Information is then collected that allows the criminal to access the actual site and the user's information.

For Business Account Users

- Remove employees from accounts they no longer use
- Limit access to what is absolutely necessary for each user
- Educate employees on safeguarding online accounts
- Conduct periodic audits of internal business controls & processes

Bank Safeguards

Below are some of the safeguards we have put in place to protect online banking customers.

- Passwords - expire on regular intervals to force password changes
- Dormant Status – accounts become dormant after an extended period of time
- Multi-factor Authentication – provides protection at various stages of login and transactions
- Security Token – a security device that generates a unique one time use code to access online banking (business accounts)
- Risk Reviews - conducted by the bank at least annually to ensure online customers are properly safeguarded
- Privacy Policy – information is protected according to federal and state mandates

Reg E Protection

Regulation E (Reg E) provides protections related to electronic transactions to consumers for consumer accounts. Internet banking losses can be recovered when detected and reported within regulation guidelines. For further information, please refer to the *Deposit Account Rules* brochure provided at the time your deposit account was opened or contact your local branch.

More Information

Check out these links for more information regarding online safety.

- Community First Bank https://www.cfbank.com/protecting-yourself-online.aspx
- www.LooksTooGoodToBeTrue.com
- Federal Trade Commission http://ftc.gov
- Federal Deposit Insurance Corporation http://www.fdic.gov
- Wisconsin Office of Privacy Protection http://www.privacy.wi.gov
- United States Government http://www.usa.gov

Contact Us

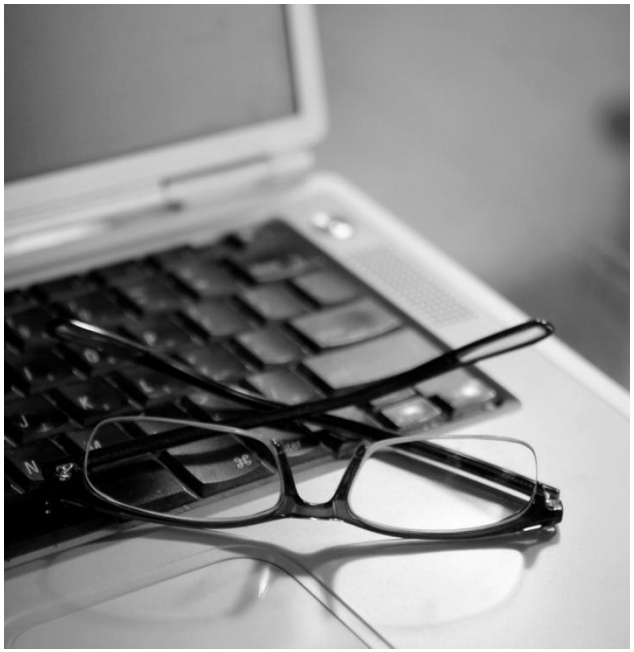
If you have concerns that your account or credentials may have been compromised, contact Community First Bank immediately.

Electronic Banking Department
Phone: 608-943-0150
Email: ebankingsupport@cfbank.com

01/2017

Online and Mobile Banking Security

Protecting Your Account



COMMUNITY FIRST BANK

"First for You"

www.cfbank.com

Boscobel
608-375-4117
Baraboo
608-356-2552
Livingston
608-943-6351
Muscoda
608-739-3154
Platteville Main
608-348-2900
Platteville Wal-Mart
608-348-6001
Reedsburg
608-524-5395
Richland Center
608-647-4029

Member FDIC