



Online Security Awareness

Community First Bank is committed to protecting the security of our customer's personal information, including when it is transmitted online. Therefore, Community First's online banking and other online services utilize advanced internet security technology to protect your personal financial information against unauthorized access. We will never request personal information via e-mail or pop-up windows. Even with the bank's robust security system in place, there are additional steps you can take to further protect your financial and personal information.

User ID and Password

To access certain online services, you have been assigned a unique user ID and password that is for your use only. Your user ID and password are designed to protect you by confirming your identity to the computer network systems. To prevent unauthorized access to your accounts, it is very important to keep your user ID and password confidential.

Here are some steps to take to protect your user ID and password:

- Do not write down your password and tape it to your computer monitor, the bottom of your keyboard, under your mouse pad, or any other place near your computer.
- Change your password periodically (monthly or quarterly).
- Change your password immediately if it becomes known, or you suspect it is known, by anyone else.
- Never give your password to anyone over the phone, regardless of the circumstances.

Selecting Strong Passwords

The objective when creating a strong password is to make it as difficult as possible for anyone to make an educated guess about what you have selected, yet, it should be developed in a manner that makes it simple to remember without writing it down.

Words to avoid when creating passwords:

Do not use your (or any family member's) name, nickname, or initials in any form (forwards or backwards spelling).

Do not use your User ID in any form.

Do not use other information that can be easily obtained about you. This includes birth dates, telephone numbers, license plate numbers, social security numbers, street addresses, or the brand of automobile you drive, etc.

Do not use all the same character (i.e. 444444) or consecutive keys on a keyboard (i.e. QWERTY).

Do not use words that would appear in a dictionary (English or other), as they can be easily compromised by password cracking programs that use electronic dictionaries.

Tips for Choosing Good Passwords

Develop a method of creating passwords that makes it easier for you to remember. You want to avoid writing it down.

You can use a line in a favorite song, poem, or movie and select the first letter of each word to create your password. Also include at least one number. For example, "The early bird catches the worm" becomes the password 1TEBCTW.

Use a word that you can easily remember, but remove the vowels and replace them with numbers. For example, the word Summer becomes the password S2MM3R.

Timeout Feature

Always log off the system after you have completed your business. As an added level of protection, Community First Bank's online banking has a timeout feature that automatically terminates your session after an extended period of inactivity.

For additional protection, access to Community First Bank's online banking will be denied or locked after three unsuccessful login attempts.

Encryption

Encryption is the process where information is transformed or coded into a form that is unreadable to anyone except those who possess the decryption key. This process prohibits unauthorized individuals from intercepting and viewing the information and is also referred to as a "secure session".

You can tell your online session with Community First Bank is secure through the following:

- An unbroken key or a locked padlock icon will appear at the bottom of your browser screen.
- The website address at the top of your browser screen will change from “http” to “https”.
- You will be required to utilize a User ID and password to gain access to the site.

Firewalls

Firewalls are an additional security mechanism the bank uses to protect your account information. A firewall acts as a barrier between the Internet and the bank’s internal network system, permitting only specific traffic to pass in and out.

Email

Email transmitted across the Internet is normally not protected and may be intercepted and viewed by others. You should, therefore, refrain from sending any confidential or private information via email to Community First Bank. We will not ask you to send confidential information to us via email, such as your user ID, password, account numbers or social security number.

Virus Protection

Community First Bank utilizes the most up-to-date technology to protect our internal systems and your personal financial information from computer viruses. Malicious viruses can sometimes be used to gain access to your personal computer. For protection of your personal system, Community First recommends you implement the following:

- Purchase and install antivirus software such as McAfee’s VirusScan or Symantec’s Norton AntiVirus to detect and eliminate potential viruses on your computer. For more information on virus detection software, visit McAfee Security or Symantec websites.
- Consider purchasing antivirus software that automatically scans for virus updates whenever you go online. If your software does not have this feature, update your antivirus software at least weekly by contacting your antivirus vendor to obtain the most current antivirus signature files.
- Do not open email attachments or downloaded files without first saving them to your hard disk (C: drive). Your antivirus software should be configured to scan each file when it is saved and when it is opened.
- Never open email attachments from individuals you do not know – simply delete them.
- Use caution with email attachments, even if you know the sender. If you were not expecting the message or if you have any suspicions, contact the sender and confirm that they did indeed send the message.

Malware Frequently Asked Questions

Malware is an attempt to trick you by popping up fraudulent login screens in order to acquire sensitive data such as your username, password, challenge questions or other information. A new version of malware targets online banking customers and primarily uses false login windows, or anything that looks different on a login window. These could be signs that your computer has been affected by malware. As a general precaution, it is best to close all other browser sessions and tabs before logging into a banking session.

1. What is malware?

Malware is a general term that refers to any kind of computer software designed to infiltrate or damage a computer system without the owner’s knowledge or consent. The word *Malware* is derived from the words **malicious** and **software**. Malware includes computer viruses, worms, Trojan horses, spyware and many other malicious and unwanted software types.

2. How does malware occur?

Malware can infect your computer through many ways, including pop-up messages that ask you to download things, infected websites, links in web pages or emails, and many other methods that can sometimes be invisible to you. Malware is often used in conjunction with a phishing scam.

3. What are the impacts of malware?

Malware, at a minimum, is a nuisance, sometimes displaying unwanted advertising or using your computer to send spam. At its worst, malware has the potential to steal personal and financial information ranging from browsing habits to email address lists to online banking passwords and even identity theft.

4. How can I protect my computer from malware?

While there is no single fool-proof method, keeping your anti-virus software up to date and running and your operating systems and applications updated with the latest patches from the manufacturers will certainly help. Other common suggestions include exercising extreme caution with email links and attachments, using firewalls to protect information on your personal computer, and watching for login windows or messages that appear strange or different which could be a sign that your computer has been affected with malware.

5. What should I do if I am affected?

First and foremost, you should contact your anti-virus software support line for assistance. Take the steps as recommended by them and always remain vigilant to the risks malware, phishing and other suspicious activities can create.