Security and Protection

At Community First Bank, you can feel confident using our banking services with comprehensive security protection. If you have received an email, text message or phone call that you want to make sure is from Community First Bank, ask us. We're happy to help. And remember – Community First Bank will never ask you to provide personal financial information over the phone, by email or text message.

Digital Security

Online Banking Security

Tips to create strong usernames and passwords:

- Choose a username that you can remember but is not easy enough for others to guess. Incorporating special characters and numbers makes your username even more secure.
- Select a username that is unique and is not used on any other website.
- Make your password sufficiently long. Passwords should contain a minimum of 14 characters. More is preferred. Choose phrases that are meaningful to you but are obscure enough not to be directly linked to your personal information.
- Make your password sufficiently complex. The shorter the password, the more important it is that you introduce things like upper- and lower-case letters, numbers and punctuation. The longer the password, the less you need to use special characters.
- Update your anti-virus, anti-spamware and anti-malware software. If your computer is compromised, the complexity and length of your password doesn't matter because it's recorded and sent to whoever is attacking you. Keeping security software and the browsers you use up to date will help prevent your computer from being compromised in the first place.
- Find out if the website you're using implements multifactor password protection. Multifactor password protection means there's more to logging in than just entering your username and password.
- Change your password often—at least every few months—and don't use the same password for every account. Also, avoid using the same password pattern over and over.

Tips to keep your information safe:

- Community First Bank will never ask for your personal or account information via email or text. Never, ever give that information out to anybody
- Never share personal information via email or text messages; especially Social Security numbers, account numbers, PIN’s, or login information
- Beware of phishing emails—these emails look like they are from your bank or other reputable companies and provide a link to verify or change your account in some way

- Beware of suspicious text messages requesting your account information via your mobile device (e.g., cell phone, smartphone, tablet)
- Keep your passwords secret, do not share passwords, do not leave passwords in an unsecured area, and change passwords regularly
- Use a different password to access your online accounts than ones you use for other applications
- Always log off your online banking session before leaving your computer
- Close all browser windows or tabs when ending your session

Mobile Security

Enabling biometric authentication, such as touch ID or Face ID, on the mobile device you use to access online banking can help prevent unauthorized access to your accounts.

Best practices to help protect your mobile device

Use Passwords, Locks and More

Always password-protect your mobile device, use the auto-lock security feature, and activate the encryption feature if one exists.

Many devices can be set so that if the wrong password is entered a certain number of times in a row, the device automatically deletes all the stored information. But don't worry — you should be able to retrieve your data from your computer if you've been synchronizing the two devices.

When creating a password, choose one that's easy for you to remember but will be difficult for others to guess. And make sure your auto-lock feature is turned on so it will kick in after a couple of minutes. That helps ensure no one will be able to use the phone or tablet without knowing your password. Also, don't share your password with anyone or tape it to your mobile device.

While encryption offers some protection and may prevent unauthorized access to your mobile data, many mobile devices don't include this feature in their operating systems. Look in the owner's manual to see if your phone has encryption, and make sure the feature is included when you purchase a new phone.

To encourage the return of a lost handset, consider writing or engraving your name and contact information — but not your password — on its back with the promise of a reward. Several applications for cell phones let you offer a reward for the return of a lost phone.

Back It Up

You should store only the information you think you'll need immediate and frequent access to in your mobile device. Remember, syncing your device to Outlook or another email application may automatically synchronize any notes in your contacts database, so pay special attention to what you have in those fields. Take care not to store usernames and passwords in the note fields.

Also make sure you have a separate record of the data, including all account numbers, passwords, phone numbers, addresses and any other sensitive information, as well as the device's make, model and serial number. Then, if your gadget is lost or stolen and you want to change your passwords quickly, you'll have the information you need at your fingertips.

Beware Fraudulent and Out-of-Market Apps

Downloading apps outside of trusted sources or jailbreaking your device can open up your phone to substantial corruptions, such as viruses or malware. Once harmful software is on your phone, it can be used to steal your personal information without your knowledge. Fraudulent apps are also on the rise; according to the FBI, US security research organizations reported that nearly 65,000 fake apps were detected on major app stores in 2018, making this one of the fastest growing sectors of smartphone-based fraud.

- Only download apps from official app stores for your device - do not download apps from unknown or unofficial sources.
- Review app permissions on any new app you download and current apps on your phone and consider deleting any with excessive permissions.
- Keep apps up-to-date as new updates are released.
- Use multi-factor authentication when possible and ensure you have strong usernames and passwords.
- Never jailbreak your device or use a jailbroken device
- If a banking app appears suspicious, call the bank at the phone number posted on their website.

Pay Special Attention to Your Tablet

Most tablets are thought of as overgrown cell phones that can be used for web browsing, video viewing and playing games. But tablets are just as capable as a phone — if not more so — of doing real work. They require the same amount of security foresight, yet few users even secure them with a password. Its larger size makes a tablet a more visible and natural target for would-be thieves. Because tablets are fully usable even without a cell phone plan, they are easier to resell on the black market.

While a phoneless tablet may not contain your cellular directory, remember that it will have everything else: from web bookmarks to all your apps (complete with account information). Tablets have been touted for banking, investing and online shopping. You probably have a few apps along these lines installed, yet minimally secured. Letting your tablet fall into the wrong hands can be as disastrous as

losing a phone.

If your mobile devices are lost or stolen:

- Call your provider to report the theft.
- File a police report (if you know it's been stolen).
- Place fraud alerts on your credit reports.
- Notify anyone whose contact or other information is stored in the phone.
- Consider using a remote wipe capability (if available) to prevent someone accessing your personal information. This feature gives you the ability to send a command to your device that will delete your data.

How to Detect Email Fraud

How to tell if an email is legitimate

Although fraudulent emails can be difficult to recognize, beware of emails that:

- Request that you click a link to a spoof website, one that looks like a real company website, including the real company's graphics and design. Since fraudulent email may even use exact wording from the real company's website, it's difficult to determine a spoof website.
- Ask you to give, confirm, or update sensitive personal information such as Social Security numbers, usernames, passwords, PIN (Personal Identification Number) or account numbers.
- Use Pop-Up windows for entering or confirming personal data (see below for more pop-up screens on secured websites.)
- Have a sense of urgency to give the information immediately, citing a specific thing that might happen. For example, your account may be closed or temporarily suspended.
- Have spelling errors and/or bad grammar. Intentional spelling errors may allow the email to get through spam filters used by ISPs (Internet Service Providers).

Even if you don't enter your personal data, by clicking on a link embedded in a fraudulent email, you may inadvertently download tracking software or viruses that track your keystrokes to gain your personal information.

Some people "test" for online fraud by entering incorrect information. If the information is accepted, then they feel they can determine that it's an email fraud. Criminals are now aware that people perform this test, and may not accept the information entered first. The best defense is not to enter any personal information at a website you link to from an unsolicited email.

How Community First Bank Protects Online Banking Customers

Community First Bank's Online Banking Platform uses a variety of security measures to ensure protection and privacy. Users must apply in person with a Government ID to obtain a user ID and temporary password. Upon entry of the user ID and password Community First Bank uses out-of-band access codes to verify that the person entering the information is correct. This is done via text message and/or email service. Access verification happens from time to time based on user IP address or length of time between logins. All information is encrypted within the online banking platform. Passwords expire and must be changed on a frequent basis. In order to protect yourself remember:

DO NOT EVER GIVE OUT YOUR USER ID OR PASSWORD TO ANYONE!

Although Community First Bank uses systems and practices designed to stop online banking fraud, this is the most practical way to protect yourself.