

Internet Banking Customer Risks & Protections

First Community Bank always strives to secure your data and continuously maintains our security to protect your information. Regulation E provides some protections to you as a consumer and customer of First Community Bank.

Under Regulation E if you suspect an electronic transaction to be fraudulent or incorrect you may be entitled to some or all your money back. If you report the suspicious activity within 2 business day your exposure will be limited to \$50.00. If you report the suspicious activity after 2 days but before 60 days of the date on your statement your exposure will be limited to \$500.00. You should report any suspicious transactions to us immediately. You may report your suspicious activity to us by writing us at: First Community Bank Attn:Customer Service P O Nox 2030 San Benito, TX 78586 or by calling us at 956-399-3331. Regulation E applies only to consumer accounts.

In addition to reporting any suspicious transactions we also recommend that you download the Trusteer Rapport software. This software helps to protect your internet banking connection with First Community Bank and helps protect your PC from malicious software. You can get more information about the Rapport software here: <https://www.fcbweb.net/protect-online-fraud-trusteer-rapport-software/>

First Community Bank **does not** make it a practice to contact our customers unsolicited and request electronic banking credentials. The only time that we may contact you is if you have download the Trusteer Rapport software and the software notifies us that you have uninstalled the software or that your PC has been infected or your PC has installed some type of malware.

For our commercial online banking customers we recommend that you perform a risk assessment on your internet banking activities. A risk assessment will allow you to evaluate any risks associated with your internet banking activities and also evaluate any controls you may have in place to mitigate these risks. The risk assessment should be performed on a regular basis and at least annually. We also recommend that that you download the Trusteer Rapport software.

In addition to our goal to preserve a safe and secure environment for your money we would like to provide some information on the possible internet threats that you need to be aware of. Some of those threats include and may not be limited to:

Malicious Software - Consists of programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

What can I do to protect myself against Malicious Software? *You can start by performing regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. If you are a windows user Microsoft offers free protection through their Microsoft Security Essentials product. It can protect your computer from viruses, spyware, and other evil software. More information can be found at <http://windows.microsoft.com/en-US/windows/products/security-essentials>. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.*

Man-in-the-Middle (MITM) Attacks - Man in the middle attacks are difficult to identify. They are a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle).

What can I do to protect myself against Man-in-the-Middle Attacks?

Again you can start by performing regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. Keeping a secured wireless and/or wired network is also a key security step. For wireless connections it is recommended to at least utilize WPA2 encryption for wireless security. Another step that you can take is to verify your account activity after you perform online transactions. Verification can also be performed by simply checking your account balance at an ATM, over the phone via our automated system or by using a second internet device (ie: cell phone, tablet). If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Man-in-the-Browser (MITB) Attacks - Like man-in-the-middle attacks, man-in-the-browser attacks are also difficult to identify. It is a form of Internet threat related to Man-in-the-Middle (MitM). This attack involves a trojan being installed that infects a web browser and has the ability to modify pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or Two or Three Factor Authentication solutions are in place. The only way to counter a MitB attack is by utilizing transaction verification.

What can I do to protect myself against Man-in-the-Browser Attacks?

Again you can start by performing regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. Keeping a secured wireless and/or wired network is also a key security step. For wireless connections it is recommended to at least utilize WPA2 encryption for your wireless network. Another step that you can take is to verify your account

activity after you perform online transactions. Verification can also be performed by simply checking your account balance at an ATM, over the phone via our automated system or by using a second internet device (ie: cell phone, tablet). If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Social Engineering - Social Engineering is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access. In most cases the attacker never comes face-to-face with the victims.

What can I do to protect myself against Social Engineering?

Since this attack depends on you releasing your private information always double check who you are sharing your private information with. Be aware that we will never contact you and ask you to disclose any of your personal information. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Phishing - This is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.

What can I do to protect myself against Phishing Attacks?

Since this attack depends on you releasing your private information always double check who you are sharing your private information with. Be aware that we will never contact you and ask you to disclose any of your personal information via email. Another step you can take is to verify both the URL of the site you may be visiting as well as the SSL certificate that site is using. The SSL certificate should be issued by a trusted certificate authority (not self-signed). If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

SMSishing (SMS phishing) - The name is derived from "SMs phISHING". SMS (Short Message Service) is the technology used for text messages on cell phones. Similar to phishing, smishing uses cell phone text messages to deliver the "bait" to get you to divulge your personal information. The "hook" (the method used to actually "capture" your information) in the text message may be a web site URL, however it has become more common to see a phone number that connects to automated voice response system.

What can I do to protect myself against SMSishing Attacks?

Since this attack depends on you releasing your private information always double check who you are sharing your private information with. Be aware that we will never contact you and ask you to disclose any of your personal information via SMS (Text message). Another step you can take is to verify both the URL of the site you may be visiting as well as the SSL certificate that site is using. The SSL certificate should be issued by a trusted certificate authority (not self-signed). If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Vishing - Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP makes formerly difficult-to-abuse tools/features of caller ID spoofing, complex automated systems (IVR), low cost, and anonymity for the bill-payer widely available. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

What can I do to protect myself against Vishing Attacks?

Since this attack depends on you releasing your private information always double check who you are sharing your private information with. Be aware that we will never contact you and ask you to disclose any of your personal information. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Keylogger - The action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

What can I do to protect myself against Keylogging?

You can start by performing regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. If you are a windows user Microsoft offers free protection through their Microsoft Security Essentials product. It can protect your computer from viruses, spyware, and other evil software. More information can be found at <http://windows.microsoft.com/en-US/windows/products/security-essentials>. For hardware based keyloggers its good practice to verify that the equipment you are using for banking activity is secured and that there are not any unusual devices attached to any of the ports. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Rootkits - Rootkits are applications that enable continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on UNIX operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware. Typically, an attacker installs a rootkit on a computer after first obtaining root-level access, either by exploiting a known vulnerability or by obtaining a password (either by cracking the encryption, or through social engineering). Once a rootkit is installed, it allows an attacker to mask the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and authorization mechanisms. Although rootkits can serve a variety of ends, they have gained notoriety primarily as malware, hiding applications that appropriate computing resources or steal passwords without the knowledge of administrators and users of affected systems. Rootkits can target firmware, a hypervisor, the kernel, or most commonly user-mode applications.

What can I do to protect myself against Rootkits?

The best way to protect against this attack is by performing regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. If you are a windows user Microsoft offers free protection through their Microsoft Security Essentials product. It can protect your computer from viruses, spyware, and other evil software. More information can be found at <http://windows.microsoft.com/en-US/windows/products/security-essentials>. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331. We may not be able to help in the removal of the possible infection, but we can perform some steps on our side to protect your information (ie: reset your account, or disable it)

Unauthorized Access - Unauthorized Access is a term that describes an attempt by an unauthorized entity to use a resource other than the authorized entity.

How can I do to protect myself from Unauthorized Access?

One way to protect your system is to enforce a system idle timeout by having your computer lock after a small amount of time. That will prevent physical access to the system and local unauthorized access. In addition to an idle timeout another protection measure is to perform regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. If you are a windows user Microsoft offers free protection through their Microsoft Security Essentials product. It can protect your computer from viruses, spyware, and other evil software. More information can be found at <http://windows.microsoft.com/en-US/windows/products/security-essentials>. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Cross-Site Scripting (XSS) - is a type of computer security vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites accounted for roughly 80.5% of all security vulnerabilities documented by Symantec as of 2007. Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

How can I do to protect myself from Cross-Site Scripting?

Ideally blocking all scripts by default and then allowing the user to enable it on a per-domain basis is effective. This has been possible for a long time in IE (since version 4) by setting up its so called "Security Zones", and in Opera (since version 9) using its "Site Specific Preferences". A solution for Firefox and other Gecko-based browsers is the open source NoScript add-on which, in addition to the ability to enable scripts on a per-domain basis, provides some anti-XSS protection even when scripts are enabled. It's always good practice to perform regular software updates/patches to your operating system and web browsers as well as anti-virus, anti-spam, anti-spyware programs. If you are a windows user Microsoft offers free protection through their Microsoft Security Essentials product. It can protect your computer from viruses, spyware, and other evil software. More information can be found at <http://windows.microsoft.com/en-US/windows/products/security-essentials>. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Password Guessing - Password Guessing is when someone gains access to your username and password by simple guessing. These attacks can be performed by an attacker manually typing in the login information until the correct credentials are entered, or by using sophisticated software to "brute-force" the correct information. Brute-forcing involves sending thousands of different logins until the correct one is finally discovered.

How can I do to protect myself from Password Guessing?

We have created some minimum requirements for your online banking passwords, using that as a baseline we encourage you to create larger more complex passwords. Longer and more complex passwords typically take exponentially more time to brute-force. Also never write your usernames or passwords down on a sheet of paper and leave it out in the open, that information can easily be copied/taken without your knowledge. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Website Spoofing - Website Spoofing is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. Another meaning for spoof is fake websites. Normally, the spoof website will adopt the design of the target website and sometimes has a similar URL. Another technique is

to use a 'cloaked' URL. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual website.

How can I do to protect myself from Website Spoofing?

Website Spoofing can be a difficult threat to detect. Most often the attackers have created sites that look identical to the “spoofed” site. We have added multiple factors of authentication to assist in identifying this treat. For example with online banking you are asked to enter a code before your password, then you are asked a security question, and finally you password is requested under a security key that you specified when you signed up for internet banking. If any of these items seem out of the ordinary there may be a chance that you are being affected by this vulnerability. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Pharming - Pharming is a hacker's attack aiming to redirect a website's traffic to another bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses – they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a neologism based on farming and phishing. Phishing is a type of social engineering attack to obtain access credentials such as user names and passwords. In recent years both pharming and phishing have been used for online identity theft information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

How can I do to protect myself from Pharming?

Pharming is similar to Website Spoofing and is a difficult threat to detect. Most often the attackers have created sites that look identical to the “spoofed” site. We have added multiple factors of authentication to assist in identifying this treat. For example with online banking you are asked to enter a code before your password, then you are asked a security question, and finally you password is requested under a security key that you specified when you signed up for internet banking. If any of these items seem out of the ordinary there may be a chance that you are being affected by this vulnerability. If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

Unencrypted Transmission of Data - Any unencrypted data that is sent out on the internet can be possibly intercepted and viewed. Secured information is typically encrypted by a SSL certificate. Without that certificate the connection between a computer and the web server is unencrypted.

How can I do to protect myself from sending Unencrypted Data?

Information shared with a website outside of an SSL session is unencrypted. One step you can take is to verify both the URL of the site you are visiting as well as the SSL certificate that site is using. The SSL certificate should be issued by a trusted certificate authority (not self-signed). If you ever feel that your private information has been compromised or that you are being targeted in this type of attack please contact our Customer Service Center directly at 1-877-399-3331.

You may contact us at anytime at 1-877-399-3331 to discuss online threats and control methods.