EMPRISE BANK®

INTERNET SECURITY INFORMATION

At Emprise Bank, we understand that the security of your personal and account information is important to you. We also understand that security is a common and legitimate concern with online banking. Fortunately, there are many steps that we can take to protect your private information from being accessed and methods you can use for ensuring your privacy.

The Reasons for Internet Security

Identity theft occurs whenever an unauthorized person takes your personal information – including social security number, account number, username, or password – and uses it to conduct fraudulent financial activity. While identity theft has been happening for years in the form of stolen checkbooks and credit card fraud, the increase of Internet-based financial transactions has created new electronic methods for obtaining access to personal data.

Malware is any malicious program that is used to collect data from your computer, capture keystrokes as you enter usernames and passwords, or corrupt programs and files. Malware is typically installed on your computer without your knowledge or consent, and includes the following types of programs:

- *Trojan horse*. A Trojan horse usually looks like an innocent program or file, but contains additional code that allows the collection, duplication, or destruction of data on your computer.
- *Adware*. While usually more annoying than malicious, adware collects data about your preferences and uses the information to create unwanted advertising, usually in the form of popups.
- *Spyware*. Spyware is software that monitors your actions on your computer.
- *Worm*. A worm is a virus that can be passed from network to network, often clogging networks and shutting down systems.

We have recently seen an increase in a malicious method of collecting personal data known as "**phishing**". Phishing usually involves an email that looks like it comes from a company or financial institution with whom you do business. It may even include a logo, a similar website address, and other identifying marks that make it look like a legitimate email from a trusted vendor. The email usually gives an alert – your information has been compromised, or your account is about to close because you haven't accessed it in a while. The email then instructs you to access a link or open an attachment, where you are taken to a new web page and asked to enter information about yourself, including name, address, account number, social security number, etc. Your personal information then becomes accessible to others.

By establishing standard security protocols, we can work to keep Internet-based financial transactions secure. Below are some ways that both Emprise Bank and our customers can prevent fraudulent activity from occurring.

Emprise Bank Security Methods

We utilize the latest technology to safeguard data through browser encryption and network monitoring. For online banking, we require unique usernames and passwords for accessing your account information. The usernames and passwords are never emailed out to you, and we will never request them when we call or email you.

Browser Encryption

Browser encryption scrambles messages exchanged between your computer and the Emprise online banking server, making it impossible for someone to "intercept" and steal your information. It works like this: when you login to online banking, your browser establishes a secure session with our server. This secure session is established using a Hypertext Transfer Protocol Secure (HTTPS) encryption.

How can you tell when your connection is secure? Look for **https://** immediately preceding the webpage address in the address bar of your browser. Or look for the padlock symbol, which can usually be found in the lower left or right hand corner of the screen, or in the address bar in newer versions of web browsers. Also, your address bar should turn green, indicating you are on a legitimate Emprise Website. We require the use of a secure,128-bit browser to encrypt information for account access and to perform transactions.

Multi-Layered Security Identification
We have implemented Extended Validation SSL Certificates to validate the exactitude of our website. The purpose of EV SSL Certificates is to identify Emprise Bank website to users as the legitimate, secure site. When logging into Online Banking in a new browser, customers will be using a One-Time Security Code to proceed into the secure browser. The security code requires the use of a home or mobile phone to complete the verification. Challenge questions have also been implemented to help verify the identity of customers. We selected questions that are hard to find using public search engines. If a customer logs in from an unregistered/ unknown computer, then they are prompted to answer a challenge question.

Network Security & Monitoring
Ensuring the security of your financial transactions is an ongoing process at Emprise Bank. We employ round-the-clock security monitoring of our systems and network. We also conduct regular third-party reviews of our security. Firewalls are used to shield Emprise Bank's systems and proprietary network from any unauthorized Internet traffic.

Email
Inquiries sent by you through our website pages use Hypertext Transfer Protocol Secure (HTTPS) and are secure. However, when we reply to your inquiry by email, our response is not secure. We will not include confidential account information in the response. To discuss specific account information, use the Secure Email link on the Emprise Bank website home page or contact an Emprise Bank Customer Service Representative by phone 316-383-4301 or 800-201-7118, or visit your local branch. You can also mail us at P.O. Box 2970, Wichita, KS 67201-2970

Customer Security Methods
There are many things that customers can do to protect themselves from identity theft.

Access ID and Passwords
When establishing your Access ID and Password(s) for online banking, we require you to use "strong" combinations that are not easily guessed by others. Strong passwords consist of a variety of uppercase and lowercase letters, numbers, and symbols. For instance, **flowers** is a weak password that might be guessed by someone who knows you like flowers. The password **Flow$283** is a stronger password that would be difficult to identify through password cracking, brute force attacks and password dictionary attacks. While this may appear to be an inconvenience to you, it makes it especially difficult to those who want to access your information illegally.

For the best security, **never** share your password with anyone. Never write it down where anyone can find it or figure out what it's for. Do not use common words that can be found in a dictionary or numbers in a series. Change your password **often**, preferably monthly.

Treat your Emprise Bank Access ID and password with more care than you use for your automated teller machine (ATM) or credit card personal identification number (PIN). With a PIN, you still need to present the card. In addition, make sure no one is physically watching you as you enter the password.

Virus Protection
Regularly updating your virus protection software can keep your computer free of viruses, especially viruses that capture keystrokes or take information off of your computer. We

recommend that enable weekly virus auto-updates. Most virus programs can be set to update automatically on a regular day of the week.

Sign-out Button
When ending an online banking session, in the upper hand right side of the webpage, click on sign out. Doing this will end your session, and you will be required to submit your username and password before entering online banking again. Shutting down your browser when you leave the computer or finish the session is also a good way of preventing others from accessing your information.

As further protection, your current session of online banking will automatically timeout after ten minutes of inactivity. To restart your session, enter your username and password at the login screen.

Always use the Sign Out button when you are accessing your online banking from a public PC or a computer that may be accessed by others. Never access online banking from a computer to which an un-trusted individual may have access.

Log On Regularly
By logging in to online banking on a regular basis, you can check account balances and transactions on your accounts to ensure that they are correct. Studies have shown that people who use online banking can identify and correct identity theft much more quickly than those who rely on paper statements. Schedule a regular time each week or day to review your transactions online and verify their legitimacy.

By taking standard precautions and employing the latest technology, we can partner with our customers to ensure that online banking is a convenient and secure tool. Studies have shown that conducting financial transactions over the internet is safer than giving your credit card to a waiter at a restaurant or reading it aloud over a cordless or mobile telephone – two activities that are generally regarded as safe. Employing the right safeguards against electronic identity theft will keep your private information protected from others.

Useful resources:
Federal Trade Commission: www.ftc.gov/bcp/edu/microsites/idtheft/
Onguard Online: onguardonline.gov/index.html

GLOSSARY
Attack: An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. An attack's effectiveness is determined by the vulnerability of the computer system and the effectiveness of monitoring and response.
Authentication: Positively identifying a user in order to allow access to a system. Authentication can also be made by users' PCs when accessing a website to verify that they are not visiting a site that has been hijacked or corrupted.
Confidentiality: Assuring information will be kept secret, with access limited to appropriate persons.
Encryption: A method of scrambling information while it moves from one source to another to prevent others from reading it.
Firewall: A system or combination of systems that enforces a boundary between two or more networks. A firewall is really a "gateway" between two networks that restricts information flow.
Identity theft: Taking personal information to conduct fraudulent financial activity.
Hypertext Transfer Protocol Secure (HTTPS) – A protocol for secure communication over a computer network which is widely used on the internet.
Malware: A generic term used to describe any form of malicious software, including viruses, Trojan horses, malicious content, etc.
Online security: Emprise Bank employs technology and monitoring to control identity theft.
Phishing: A "phishing" email may look exactly like a legitimate email from a bank or financial institution you regularly do business with. However, a phishing email will typically ask you to visit a web link, where you will be asked to fill out items such as name, address, account numbers, credit card numbers, etc.

Popup: A new browser window that appears – unrequested by you – on your screen. Commonly used for advertisements.
Secure browser: An Internet browser that has SSL encryption version 3.0 or higher. A secure browser is used to conduct secure financial transactions over the internet.
Secure Socket Layer: A form of encryption that protects information from being transmitted over the Internet, and to prevent tampering while the information is in transit.
Secure Transaction: A transaction that is protected from outside tampering.
Sensitive information: Includes identifying items such as account numbers, usernames, passwords, PINs, and social security numbers.
Spam: Unsolicited "junk" email sent to large numbers of people to promote products or services.
Spam filter: Blocks spam from being delivered into your email inbox.
Spyware: Spyware is software that is installed on your computer and monitors your activity, without your knowledge or consent. Spyware may give you unwanted advertising in the form of pop-ups, or may collect personal information about you.
TLS: A form of encryption that ensures privacy between communicating applications and their users on the internet. It prevents third parties from eavesdropping or tampering with any messages.
Trojan Horse: An apparently useful and innocent program that allows the unauthorized collection, use, or destruction of data.
Virus: A program that can "infect" other programs by modifying them.
Virus Protection (also Anti-Virus Software): Software that scans items as they are received onto your computer to check for viruses. Anti-virus software will alert you when a virus has been received and quarantine it. These should be updated weekly to ensure the latest protection against viruses that might capture data or record keystrokes.
Worm: Program that spreads itself from network to network, often "clogging" information systems as it spreads.

Updated September 2017