Security

Whether it's the safety of your personal financial information or identity protection, Third Coast Bank SSB is committed to keeping your information safe and secure. We employ security measures that comply with federal regulations and maximize the security for your online banking activities.

Threats

Social Engineering\Phishing

What is Social Engineering?

Social Engineering is a technique used to obtain or attempt to obtain secure information by tricking an individual into revealing the information.

The basic goal of social engineering is to gain unauthorized access to personal\information or systems in order to commit fraud, network intrusion, identity theft, or simply to disrupt and\or compromise computer systems.

Please notify the Bank at 713.446.7000 if you feel you have been a victim.

Phishing refers to attempts to steal personal financial information, such as credit card numbers, account usernames\passwords, and social security numbers, through fraudulent e-mails, phone calls (vishing), text messages (smishing) and websites that will be used for fraudulent purposes.

How Phishing Works

- You receive an e-mail, call, or text message which appears to originate from a bank, financial institution or other well-known or reputable entity
- The fraudulent message usually provides a link and an urgent message that directs the user to visit a website that looks legitimate and authentic or provides a number to call where they must verify or update personal information, such as passwords, credit card information, social security number and bank account numbers which the legitimate organization already has
- The website, however, is bogus and set up only to steal the user's information

How to Avoid Phishing

- Do not reply to these messages or visit these websites included in the e-mails warning that your account will be shut down\closed unless your personal information is confirmed
- Never send sensitive data such as passwords, account numbers or social security numbers in response to an e-mail, a text message or a phone call
- Do not reveal personal\financial information or passwords to anyone
- Do not click on links in e-mails. Go directly to the company’s main site to login
- Contact the company in the e-mail by using a telephone number or web address you know to be genuine
- Before submitting personal\financial information through a website, look for the "lock" icon on the browser status bar to ensure your information is secure during transmission
- Report suspicious activity to the Federal Trade Commission at www.ftc.gov

Corporate Account Takeover

Corporate Account Takeover (CATO) is a type of business identity theft where cyber criminals\thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions.

Call the Bank immediately at 713.446.7000 if you believe that your Third Coast Bank SSB account has been compromised.

Malware

Malware is software that gets installed on your machine and performs unwanted tasks. Malware programs can range from being simple annoyances (pop-up advertising) to causing serious computer invasion and damage.

Some categories of malware are:

- **Virus**: Software that can replicate itself and spread to other computers or that are programmed to damage a computer by deleting files, reformatting the hard disk, or using up computer memory
- **Adware**: Software displays pop up ads or redirects your browser when you're connected to the internet
- **Spyware**: Software that gathers information and transmits it to interested parties. Information gathered includes visited websites, browser/system information, and your computer's IP address
- **Ransomware**: Software that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the cyber criminals\malware operators to remove the restriction.
- **Browser hijacking software**: Advertising software that modifies your browser settings, creates desktop shortcuts, and displays intermittent advertising pop-ups. Once a browser is hijacked, the software may also redirect links to other sites that advertise, or sites that collect web usage\login information

Keystroke Logging (Keylogger)

A program that captures and transmits the keys struck on a keyboard. The keylogger is usually installed from malware delivered by a phishing e-mail or some other malicious attack to spy on what a user is typing, such as usernames and password combinations.

Protection

Firewall and Malware Protection

A firewall is a barrier between the Internet and your network\computer that controls access to the resources of a network. Typically means that the only traffic allowed onto the network is defined; all other traffic is denied. Using a firewall is highly recommended. However, a firewall isn't sufficient on its own to guarantee security, but it is the first line of defense.

A firewall provides limited or no protection against:

- If you give permission for other computers to connect to yours
- If it is switched off, disabled or contains many exceptions or open ports
- Against most viruses
- Against spam
- Against spyware installations
- Against any kind of fraud or criminal activity online
- If you or a virus has created a back door through the firewall
- If a hacker has the password for the firewall

- Against people with physical access to your computer or network systems
- Against malicious traffic that does not travel through it, for example via a poorly configured wireless network
- Against attacks after a network has been compromised
- Against traffic that appears to be legitimate
- Against phishing

Anti-virus and Anti-malware software are classes of programs that help prevent, detect and remediate virus\malware infections on computers systems.

Wi-Fi Security

Only connect to Wi-Fi networks that you absolutely trust. Turn off the automatic connect function on your phone. Never access online services from public Wi-Fi such as restaurants, cafes, public libraries, etc.

Shopping Safely Online

Online shopping has become a popular way to purchase items without the hassles of traffic and crowds. However, the internet has its risks, so it is important to take steps to protect yourself when shopping online.

Password Tips

We all know that passwords are a pain to remember, but in the long run, you will be happy that they are required. There are many malicious hackers out there in the world today and having a complicated password is just one step to making it even more difficult for them to get your personal information.

Some tips on protecting yourself with your passwords are:

- Create strong passwords with at least 8 characters that includes a combination of mixed case letters, numbers and special characters
- If the form is case sensitive, make some characters upper case and some lower case
- Do not use generic passwords such as the word password, 123456789, any part of your name, address, birthday, phone number
- Use a different password for each website that is accessed
- Change the passwords a least several times each year
- Never share username and password information with anyone
- Never give out your password to anyone (not even to the bank)
- Do not write your passwords down to where someone could easily see them

Best Practices to Help Protect Your Personal Information

- Be suspicious of e-mails purporting to be from banks, financial institution or government agencies requesting account information or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening attachments or clicking on web links in suspicious emails could expose your system to malicious code that could hijack your computer or steal your credentials. Third Coast Bank SSB will never contact you and request your passwords.
- Install a dedicated firewall
- Install virus/malware protection on all computer systems and ensure they are updated regularly
- Computers and servers should be patched regularly
- Consider spyware detection programs
- Verify use of a secure session (https, not http) in the browser for all online banking sites
- Avoid using automatic log-in features that save usernames and passwords for online banking
- Never leave a computer unattended while using any online banking service

- For businesses that conduct online transactions, it is recommended that commercial online banking activities be carried out from a stand-alone, hardened and completely locked down computer from which e-mail and web browsing are not possible
- Make frequent backups of your data
- The best protection you provide for yourself is to never give out personal information over the Internet
- Remember, **Third Coast Bank SSB** will NEVER ask for your debit card PIN or online account passwords
- Treat your mobile device with the same level of care as you would a credit card. If it is lost or stolen and you have not protected the device adequately, you may be at risk
- Password-protect your mobile device

For more information on best practices to maximize the security of your online banking experience and activities, see the FDIC information linked below (please note hyperlinks have been removed, please copy and paste the links below into a new browser window to open):

https://www.fdic.gov/consumers/consumer/news/cnwin18/