Banking Security Tips

When it comes to keeping your personal and financial information safe, it's important to be proactive. Follow these tips to help protect yourself/company from fraud and identity theft.

Protect your identity

Safeguard your personal and financial information so that it doesn't fall into the wrong hands.

Identity Protection Tips

- Carry only necessary information with you. Leave your Social Security card and unused credits cards in a safe and secure location.
- Do not provide your Social Security number unless absolutely necessary.
- Make photocopies (front and back) of vital information you carry regularly and store them in a secure place, such as a safety deposit box. Then, if your purse or wallet is lost or stolen, you have contact information and account numbers readily available.
- If you are uncomfortable with a phone call that was not initiated by you, hang up or ask for the purpose of the call. Then contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit or credit card.
- Never provide payment information on a call that you did not initiate.
- Replace paper invoices, statements and checks with electronic versions, if offered by your employer, bank, utility provider or merchant.
- If you have free online account access with 5StarOnlineBanking or 5StarOnlineBusinessBanking, you can reduce paper statements by signing up for Bill Pay and free online statements.
- Shred documents containing personal or financial information before discarding. Many fraud and identity theft incidents happen as a result of mail and garbage theft.
- Review your credit report at least once a year to look for suspicious or unknown transactions. You can get a free credit report once a year from each of the three major credit bureaus at www.annualcreditreport.com.
- Promptly retrieve incoming mail and place outgoing mail in a U.S. Postal Service mailbox, instead of your home mailbox, to reduce the chance of mail theft. Consider paperless options for your bills and financial statements.

- Know your billing and statement cycles. Contact the company's customer service department if you stop receiving your regular bill or statement.

Protect your accounts

There are many steps you can take to secure your checking, credit card, and debit card accounts. These tips can help get you started.

Checking Account Security Tips

- Report lost or stolen cards and checks immediately.
- Review account statements carefully. Regular account review helps to quickly detect and stop fraudulent activity. Ask about suspicious charges.
- With 5StarOnlineBanking or 5StarOnlineBusinessBanking, you can monitor your account online any time and as frequently as you like.
- Limit the amount of information on checks. Don't print your driver license number or Social Security number on your checks.
- Store new and cancelled checks in a safe and secure location.
- Carry your checkbook with you only when necessary.
- Use tamper-resistant checks. 5StarBank checks include many safety features such as tamper-resistant packaging and chemically sensitive paper to deter alterations.

Credit Card and Debit Card Security Tips

- Always keep your credit or debit card in a safe and secure place. Treat it as you would cash or checks. Contact 5StarBank immediately at 1-800-776-2265 (BANK) if your card is lost or stolen, or if you suspect unauthorized use.
- Do not send your card number through email, as it is typically not secure.
- Do not give out your card number over the phone unless you initiated the call.
- Regularly review your account statements as soon as you receive them to verify transactions. Contact 5StarBank immediately if you identify any discrepancies.
- If you have forgotten your PIN or would like to select a new one, please visit your nearest 5StarBank location.
- To protect your account, 5StarBank recommends you change your Personal Identification Number (PIN) regularly.

- When selecting a PIN, don’t use a number or word that appears in your wallet, such as name, birth date, or phone number.
- Ensure no one sees your PIN when you enter it. Memorize your PIN. Don’t write it down anywhere, especially on your card, and never share it with anyone.
- Cancel and cut up unused credit and other cards. If you receive a replacement card, destroy your old card.
- Shop with merchants you know and trust.
- Make sure any internet purchase is secured with encryption to protect your account information. Look for secure transaction symbols such as a lock symbol in the lower right-hand corner of your web browser, or “https://…” in the address bar of the website. The “s” indicates "secured" and means the web page uses encryption.
- Always log off from any website after a purchase transaction is made with your credit or debit card. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.
- Safe-keep or securely dispose of your transaction receipts.

Be safe online and on your mobile device

Whether you’re sending emails, shopping online, using social media, or just surfing the Web, it’s important to keep your account information and identity secure. Follow these tips to avoid compromising your information.

Online Security Tips

- Do not use your Social Security number as a username or password.
- Use a unique username and password for your 5StarBank account, update them regularly, and do not use any part of your email address as your username or password.
- Protect your online passwords. Don’t write them down or share them with anyone.
- Protect your answers to security questions. Do not write down or share your answers with anyone. 5StarBank will never ask you to provide answers to security questions via email.
- Use secure websites for transactions and shopping. Shop with merchants you trust. Make sure internet purchases are secured with encryption to protect your account. Look for secure transaction signs like a lock symbol in the lower right-hand corner of your browser or “https” in the address bar.

- Social media is increasingly popular, but it's a good idea to keep certain personal information private. Avoid sharing personal details that are used by financial institutions to identify you, such as your birth date, home address, mother's maiden name, schools attended/mascots and pet's name. Fraudsters may use this type of information to help gain access to an account since they are common answers to security questions.
- Always carefully review the privacy options for any social network you join. The privacy options and tools for social networks can be complex and should be reviewed carefully so that there is no disclosure of information you meant to remain private.

Business Banking Security Tips

- Dual Control is a powerful way to protect your accounts and money when it comes to ACH or wire privileges.
- Log off after every online session. Never leave a session open.
- Protect your user name and password information.
- Don't allow access to accounts to which an individual sub user does not need to access.
- Don't request privileges on accounts (like Wire or ACH) which you rarely or never use to transact.
- Include your cell phone number as a means to receive security alert notifications in addition to email.
- Ensure your computer operating system, software; browser version and plug-ins are current. Before downloading an update to your computer program, first go to the company's website to confirm the update is legitimate.
- Install a firewall on your network and keep anti-virus software installed and updated.
- Consider having a security audit conducted on your network to point out and correct any issues that may cause problems.
- Review the privileges of sub-users at least once annually.

Email Security Tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.

Fraudulent emails (phishing)

Phishing is usually a two-part scam involving emails and spoof websites. Fraudsters, also known as phishers, send an email to a wide audience that appears to come from a reputable company. This is known as a phish email.

In the phish email, there are links to spoof websites that imitate a reputable company's website. Fraudsters hope to convince victims to share their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately or a need to communicate with you for your own safety or security. Once obtained, your personal information can be used to steal money or transfer stolen money into another account.

Use caution if you receive an email expressing an urgent need for you to update your information, activate your online banking account, or verify your identity by clicking on a link. These emails may be part of a phish scam conducted by fraudsters to capture your confidential account information and commit fraud. Never open attachments, click links, or respond to emails from suspicious or unknown senders. If you receive a suspicious email that appears to be from 5StarBank, report it and delete it.

How fraudsters obtain email addresses

Fraudsters obtain email addresses from many places on the Internet. They also purchase email lists and sometimes guess email addresses. Fraudsters generally have no idea if people to whom they send banking-related phish emails are actual bank customers. Their hope is that a percentage of those phish emails will be received by actual bank customers.

If you receive a fraudulent email that appears to come from 5StarBank, this does not mean that 5StarBanks computer systems have been breached.

Fraudulent websites (phish or spoof websites)

Fraudsters may attempt to direct you to spoof websites via emails, pop-up windows or text messages. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you got to the site. Use caution if you may have followed a link in a suspicious email, text message, online chat or other pop-up window requesting your personal or account information.

Text-message phishing (smishing)

A phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device. This tactic is also referred to as **smishing**, which is a combination of SMS and phishing. The purpose of text message phishing is the same as traditional email phishing: convince recipients to share their confidential information.

Never take action on a request for your personal or financial information, including account numbers, passwords, Social Security number or birth date. If you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information, on a website, do not respond and delete it. These messages may be part of a phishing scam conducted by fraudsters in an attempt to capture your confidential account information and may be used to commit fraud.

Telephone or voice phishing (vishing)

Known as **vishing**, or voice phishing, this tactic is a phishing attempt made through a telephone call or voice message. Fraudsters may have the ability to spoof their caller ID so it could appear that the telephone call is coming from a legitimate company. Fraudsters may also have identifying customer information, such as your name, which they may use to make the call appear more authentic.

If you are uncomfortable with a phone call that was not initiated by you, ask for the purpose of the call and then hang up. Then, contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit or credit card.

Paper mail or fax phishing

Some fraudsters still use low-tech methods to obtain your personal and financial information. Phishing attempts can be made through regular mail or fax machines. If you are suspicious about a piece of mail or fax you have received requesting personal or financial information, you should discard it. If you responded to a suspicious mailing or fax and provided confidential information, contact the company the mail or fax appears to be from. Use a legitimate source such as the phone number listed on the company's website, billing statement, or on the back of your ATM, debit or credit card to determine if your information was compromised.

Pop-up windows

Fraudsters may use pop-up windows – small windows or ads – to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. If you encounter a suspicious pop-up window, close it. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer.

- **Mobile Security Tips**

When you use a mobile device to access your accounts, keep these tips in mind:

- Use the security functions that come with your device, such as the keypad lock or phone lock function when it is not in use, or the “find my phone” or “wipe out memory” functions if it is lost.
- Frequently delete text messages from your financial institution, especially before loaning out, discarding, or selling your mobile device.
- Keep your account numbers, passwords, Social Security number and date of birth private. Never share your personal or financial information in a text message, phone call or email.
- If you lose your mobile device or change your mobile phone number, call customer service at 1-800-776-2265 (BANK)
- Avoid storing your banking password or other sensitive information on your smartphone or in an app where it could be discovered if your phone is stolen.
- When you finish banking on your mobile device or using the 5StarBank app, always log off and not just close the browser or app. For your security, 5StarBank’s mobile apps and mobile banking site will automatically log you off after 10 minutes of inactivity.
- To ensure the highest level of protection, keep your mobile operating system up to date and do not alter or "jail break" your mobile device. If you have concerns about an update to your mobile device, visit the company’s website to confirm that the update is legitimate.
- Be cautious when using public hotspots. Carefully consider your Wi-Fi and Bluetooth connection settings, even at a trusted retailer, as fraudsters can spoof the name of reputable hotspots.
- Download banking applications from reputable sources only to ensure the safety of your account information. Download the 5StarBank app by searching “5StarBank” in your phone’s app store.
- If you have suspicions about the authenticity of a 5StarBank mobile banking app, access your account through our mobile banking site at m.5StarBankus.com.
- Treat QR codes with the same suspicion as you would any URL or link you find in an email. Much like links in email, QR codes can be used by fraudsters to send you to websites that may request your personal and financial information or could corrupt your mobile device.

- Use caution on which QR codes to scan, as some may have been tampered with if placed in a public place.
- Use a QR code scanner from a reputable source that will check links for malicious content. This capability can be found in the app description before downloading.

Computer Security Tips

- Avoid downloading programs from unknown sources.
- Ensure your computer operating system, software; browser version and plug-ins are current. Before downloading an update to your computer program, first go to the company's website to confirm the update is legitimate.
- Install a personal firewall on your computer and keep anti-virus software installed and updated.
- Be wary of conducting online banking activities on computers that are shared by others. Public computers should be used with caution. Online banking activities and viewing or downloading documents (statements, etc.) should be conducted, when possible, on a computer you know to be safe and secure.
- Configure your devices to prevent unauthorized users from remotely accessing your devices or home network. For example, if you use a home wireless router for your home internet connection, follow the manufacturer's recommendations to configure the router with appropriate security settings.