Fraud Prevention 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 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 at home 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 safe 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 or personal 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 FinWise Bank or FinWise Bank Business Banking, 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. Get a copy at any time directly from:
  - Equifax: **1-800-685-1111** or www.equifax.com
  - Experian: **1-888-397-3742** or www.experian.com
  - TransUnion: **1-800-916-8800** or www.transunion.com

- Subscribe to a daily **credit monitoring service**, which includes a personal credit report and quarterly updates from up to all three major credit bureaus. (Restrictions and fees apply; refer to terms and conditions.)
- 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.

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 FinWise Bank immediately at 1-801-501-7200 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 FinWise Bank immediately if you identify any discrepancies.
- If you have forgotten your PIN or would like to select a new one, please visit us.
- To protect your account, FinWise Bank recommends you change your Personal Identification Number (PIN) every six months.
- 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.
- Change your usernames and passwords regularly and use combinations of letters, numbers, and special characters such as # and @. Do not use your FinWise Bank credentials for other online accounts.
- To change your FinWise Bank username or password:
  - Sign on to an online banking session.
  - Click on the My Settings tab.
  - Under My Profile, select **Update Username** or **Update 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. FinWise Bank 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.

Email Security Tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- If you receive a suspicious email that you think is a phish, do not respond or provide any information.
- If you respond to a phish email with personal or account information, contact FinWise Bank at 801-501-7200.

Mobile Security Tips

When you use a mobile device for browser or text-based account access, keep these tips in mind:

- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password-protect your device to make it more difficult for someone else to view your information.
- 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, remove the old number from your mobile banking profile at the My Settings page within online banking or call customer service at **801-501-7200**.
- 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 online, always log off. FinWise Bank's smartphones apps, iPad apps and mobile banking site will automatically log you off after 10 minutes of inactivity. This reduces the risk of others accessing your information from your device.

- Keep your mobile operating system up to date to ensure the highest level of protection. Before downloading an update to your mobile device be sure to go to the company's website to confirm 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.

    Applications are programs you can download to your mobile device. Applications or "apps" let you monitor your finances and conduct certain transactions are increasing in popularity.

- Download banking applications from reputable sources only to ensure the safety of your account information. Download the FinWise Bank app by searching "FinWise Bank" in your phone's app store, or visit www.finwisebank.com on your phone's browser.
- For your security, sign off when you finish using a FinWise Bank app rather than just closing it.
- If you have suspicions about the authenticity of a FinWise Bank mobile banking app, access your account through our mobile banking site at www.finwisebank.com.

QR codes (quick response codes) are two-dimensional barcodes that can be scanned with a mobile device to provide easy access to online information. 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.

- Treat QR codes with the same suspicion as you would any URL or link you find in an email.
- Use caution on which QR codes to scan, as some may have been tampered with if placed in a public location.
- 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.