HomeTown Bank of Alabama Security Tips

BANK SECURITY

It is the policy of HomeTown Bank of Alabama to protect your information to the best of our ability. This information includes but is not limited to your name, address, social security number, phone number, transaction histories, or any other information that would fall under the Gramm–Leach–Bliley Act (GLBA Data). In the unlikely event you fear any of the above mentioned items may have been compromised please contact us immediately at (205) 625-4434.

Thieves will stop at nothing to get your personal information and card data. Their scams can be clever, but not clever enough, if you know how they work and how to avoid them. We've highlighted a few of the ways fraudsters and identity thieves try to get your information.

TRENDING SCAMS

Thieves are always looking for the latest and greatest way to obtain your information. Here are a couple of scams that are trending now:

FAKE CHECK SCAM: An official-looking envelope arrives in the mail with a check or money order for $20,000 inside. The letter says you have won $4 million in a sweepstakes or lottery. You just need to wire $3,000 for taxes to claim the rest of your winnings. Is this your lucky day? NO! It is a fake check scam that will cost you thousands. No matter the story, fake check scams always involve someone giving you a genuine-looking check or money order and asking you to wire money somewhere in return. After you deposit or cash the check or money order and send the money, you learn that it was phony. Now the crook has the money and you owe it back to your bank. Your bank confirms that the check or money order is legitimate before letting you have the money, right? Wrong. Federal law allows you to get the cash quickly, usually within 1-2 days. But your bank cannot tell if there is a problem with a check or money order until it goes through the system to the person or company that supposedly issued it. This can take weeks. YOU are responsible because you are in the best position to know if the person who gave you the check or money order is trustworthy.

ELDER ABUSE: Financial fraud is the fastest growing form of elder abuse. Broadly defined, financial elder abuse is when someone illegally or improperly uses a vulnerable senior's money or other property. Most states now have laws that make elder financial abuse a crime and provide ways to help the senior and punish the scammer. Elder financial abuse is tough to combat, in part because it often goes unreported. You can protect yourself or your loved ones from financial elder abuse by becoming familiar with the most common scams and learning what to do if you suspect foul play. Common scams are:

- Telemarketing or mail fraud. Scammers also use the phone to sell seniors goods that either never arrive or are worthless junk.
- Getting unauthorized access to funds. In "Sweetheart Scams," alleged suitors woo older people, convincing them that love and care are their motivations for being included on bank accounts or property deeds; the suitors usually disappear along with the property.

- Charging excessive amounts of money. Smooth-talking scammers first convince seniors that they need some goods or services, and then seriously overcharge them, often hiding the high cost in extravagant schemes involving interest and installment payments. This tactic is often used for products that many older people might find essential to their quality of life, such as hearing aids and safety alert devices.
- Getting money or property through undue influence or fraud. Many seniors have been duped into parting with their homes or other property because a scammer convinces them it is for their own good.
- Using fraudulent legal documents. Many scammers cloak their actions in legal authority, procuring a power of attorney, will or other legal document giving them access to a senior's property. They get seniors to sign these documents by lying to, intimidating, or threatening the seniors.
- Faking an injury scenario. In this situation, a scammer claims to have a connection to law enforcement and tells an elder that a child or other close family member has been seriously injured or is in jail. The scammer then convinces the senior to give him or her money for medical treatment or bail.
- Doing unsolicited home repair work. Typically working in teams of two or more, scammers scour neighborhoods with a high concentration of older residents, or even track recent widows and widowers through obituaries and death notices, then appear on their doorsteps claiming to spot something in need of fixing -- a hole in the roof or clogged drainpipe, for example. The scammers demand payment up front, and then often claim that their initial investigation reveals a more serious problem, with a more expensive solution.

PHISHING

Phishing is when fraudsters pretending to be from well-known companies, organizations, or government agencies contact consumers and try to trick them into revealing their personal information. That information is then used to commit fraud like opening new accounts in your name or taking over existing accounts like online banking or iTunes. It can happen over the phone, on email or even through text messages. Protect yourself with these quick tips:

- Be on your toes. Only open emails, attachments, and links from people you know.
- Don't believe what you see. It's easy to steal the colors, logos and the header of an established organization and make emails appear legitimate.
- Avoid sharing. Don't reveal personal or financial information in an email, text or over the phone.
- Pay attention to a website's URL. Hover over any links to see where they lead.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.
- Keep a clean machine. Make sure you keep your anti-virus software up to date.

If you believe your card data may have been compromised in a data breach, contact HomeTown Bank of Alabama immediately.

EMAIL

HomeTown Bank of Alabama does not contact customers via email requiring you to install software or requesting you provide personal information such as a PIN or passwords.

- Consider all email requests for personal information to be suspicious
- Do not respond to such emails or enter information on questionable websites
- Report suspicious emails or websites to HomeTown Bank of Alabama at 205-625-4434

COMPUTER & ONLINE BANKING SECURITY TIPS

From spyware to shady merchants, the threat of online fraud is real, but you are the best line of defense. The key to combating online fraud is knowing what threats exist and taking easy steps to beat them. To prevent online fraud:

- Keep current with your software and virus protection
- Look for the green box with a lock in the address bar. This signals a secure site.
- Create strong passwords (this means using capital and lowercase letters, numbers AND symbols).
    - Avoid using commonly available identifying information for passwords such as birthdays, children's names, etc.
    - Avoid using the same password across multiple sites. Although this sometimes makes it easier for you it also makes it easier for crooks to steal from you.
- Ignore emails from senders you don't know
- Use your pop-up blocker
- Download files only from sites you know
- Entities such as the FDIC, IRS, NACHA, etc. do not contact business customers to request software installation or to ask for customer's access credentials. If you receive any such request please contact HomeTown Bank of Alabama immediately.

CORPORATE ACCOUNT TAKEOVER (CATO)

Corporate Account Takeover occurs when a criminal obtains electronic access to your bank account and conducts unauthorized transactions. The criminal obtains electronic access by stealing the confidential security credentials of your employees who are authorized to conduct electronic transactions (wire transfers, Automated Clearing House-ACH, and others) on your corporate bank account.

There are several methods being employed to steal confidential security credentials. *Phishing* mimics the look and feel of a legitimate financial institution's website, e-mail, or other communication. Users provide their credentials without knowing that a perpetrator is stealing their security credentials through a fictitious representation which appears to be their financial institution. A second method is *Malware* that infects computer workstations and laptops via infected e-mails with links or document attachments. In addition, malware can be downloaded to a user's workstation or laptop from legitimate websites, especially social networking sites. Clicking on the documents, videos, or photos posted there can activate the download of the malware. The malware installs key-logging software on the computer, which allows the perpetrator to capture the user's ID and password as they are entered at the financial institution's website.

What can business customers do to protect themselves (best practices)?

- Education is Key – Train your employees
- Implement dual controls for high-risk online functions
- Secure your computer and networks

- Limit Administrative Rights - Do not allow employees to install any software without receiving prior approval.
- Install and Maintain Spam Filters
- Install & maintain real-time Anti-Virus & Anti-Spyware Desktop Firewall & Malware
- Detection & Removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.
- Install security updates (patches) to operating systems and all applications as they become available.
- Block Pop-Ups
- Use strong password policies
- Do not open attachments from e-mail - Be on the alert for suspicious e-mail
- Do not use public Internet access points
- Monitor and Reconcile Bank Accounts Daily - especially near the end of the day
- Note any changes in the performance of your computer - dramatic loss of speed, computer lock-ups, unexpected rebooting, unusual pop-ups, etc.
- Make sure that your employees know how and to whom to report suspicious activity – both at your Company & your Bank
- Use multi-layer security

Contact the Bank if you:

- Suspect a Fraudulent Transaction
- If you receive an e-mail claiming to be from the Bank and it is requesting personal / Company information

The Bank will NEVER ask for sensitive information, such as Account Numbers, Access IDs, or Passwords via e-mail.

Incident Response Plans

Since each business is unique, customers should write their own *Incident Response Plan*. A general template would include:

1. The direct contact numbers of key bank employees (including after-hours numbers);
2. Steps the accountholder should consider to limit further unauthorized transactions, such as:
    a. Changing passwords;
    b. Disconnecting computers used for Internet Banking;
    c. Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
    d. Noting information the accountholder will provide to assist the bank in recovering the accountholder's money; e. Contacting their insurance carrier; and
    e. Working with computer forensic specialists and law enforcement to review appropriate equipment.

TRAVEL

Don't let fraud ruin your business or pleasure travels! Take these few easy measures before you leave:

- Tell your card issuer where you're headed and for how long
- Note card numbers, balances and issuer phone numbers and keep them in a safe place
- Save and check all receipts against your statement
- Don't leave cards unattended

RETAIL/ATM

Accepted across the world, more convenient and safer than cash, payment cards have transformed how we shop and bank. But thieves may try to steal your card information and use it for unauthorized charges. Make sure you make these transactions in ways that reduce your risk of fraud. To help stop retail/ATM fraud, remember:

- Review receipts before you sign
- Monitor your statements
- Keep copies of ATM and sales receipts for your records
- Be aware of your surroundings
- Guard your PIN from "shoulder surfing"
- Report missing cards immediately

ATM SKIMMING

Automated Teller Machine or ATM skimming is a fraud scheme to steal personal information from ATM users. A skimmer is a piece of equipment which is installed by scammers on the ATM or wherever cards are swiped like gas stations to read a cardholder's electronic account information stored on the magnetic stripe on the back of the card when the card is inserted into the skimming device.

Below are a few precautions you can take to help prevent you from falling victim to ATM Skimming:

- Familiarize yourself with the look & feel of your bank's ATM
- Inspect the ATM for unusual or non-standard appearance
- Is there anything unusual (card reader, area above the screen)?
- Report any unusual appearance immediately to Hometown Bank of Alabama at 205-625-4434
- Always use your hand to shield your PIN when entering it

MAIL AND PHONE

Fraudsters can send official-looking letters or pose as representatives from HomeTown Bank of Alabama, other financial institutions/credit accounts or even charities. If asked to provide your account number or other personal information in the mail or by phone, be wary of fraud. A few tips can help you beat phone fraud:

- HomeTown Bank of Alabama never calls or writes account holders for personal account information
- Never provide information unless you initiated the communication
- Don't feel obligated to provide card numbers by phone
- Get details—If the caller can't answer, it's not legitimate
- Rather than asking for a "call back number," research the caller on your own along with their legitimate phone number

- Report requests for personal information to your card issuer by calling the number on the back of your card as well as by calling HomeTown Bank of Alabama at 205-625-4434

You can combat fraud by mail, too:

- Beware of notices announcing that you've won a prize for a contest you did not enter
- Notify your post office if you change address
- Make sure your mailbox is secure
- Collect your delivered mail; don't let it sit in the mailbox too long
- Have your mail held when on vacation

AT HOME

Did you know that half of all identity theft is committed by individuals with legitimate access to your home such as live-in caregivers, relatives or renovation crews? Home is a safe place, and here are a few tips to help keep it that way:

- Monitor your accounts often
- Check your credit report to make sure it's correct
- Store important documents securely

IDENTITY THEFT

If thieves obtain your driver's license or Social Security number, they can pretend to be you and potentially open bank accounts, order credit cards, write bad checks and obtain loans. They can also ruin your credit score and make it hard to obtain credit in the future. Identity thieves use a variety of tactics, even "dumpster diving" through your trash for personal information. To help stop identity theft:

- Monitor card and account statements frequently
- Report missing cards immediately
- Cancel all inactive accounts
- Do not volunteer any personal information unless necessary
- Sign new cards upon receipt
- Shred sensitive documents before disposing of them
- Install anti-virus and anti-spyware software
- Change passwords regularly

Reporting identity theft/fraud

At HomeTown Bank of Alabama we are committed to helping you protect yourself from fraud. If you suspect that you have been a victim of fraud or identity theft it is important to take immediate action. Contact HomeTown Bank of Alabama immediately at 205-625-4434. Contact the Federal Trade Commission's Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357).

Notifying credit bureaus

It is highly recommended that you contact the three national consumer reporting agencies if you believe you have been a victim of identity theft. Ask each agency to place a "fraud alert" on your credit report and to send you a copy of your credit file.

Equifax – 1-800-465-7166
www.equifax.com

Experian – 1-888-397-3742
www.experian.com

TransUnion – 1-800-680-7289
www.transunion.com