ONLINE BANKING BEST PRACTICES

(full version)

The Bank of San Antonio has robust technology and procedures in place to prevent unauthorized access to your account. In recent months, the financial services industry has seen small and medium-sized businesses suffer data security breaches resulting in fraudsters gaining unauthorized access to the company's online banking platform. The Bank of San Antonio continues to monitor and adjust our security infrastructure based on the latest threats.

Due to many banks (such as The Bank of San Antonio) having more sophisticated IT security systems, the computer criminals are turning away from the tightly secured bank computers and are looking toward potentially weaker places in terms of security to attack: **the bank client's computer systems**. More and more attacks are being committed against small and medium-sized businesses because their computer security is viewed as more lax than large companies/banks, and they typically maintain a higher account cash balance than individual personal accounts.

Furthermore, these extremely sophisticated criminals know that a bank's computer systems are designed to thwart unauthorized users. So, they find ways to fraudulently APPEAR as a legitimate user (through identity theft, obtaining insider information, spying, etc. Since the bank strives to make the online experience easy for our clients, exposure to this type of fraud is especially risky to businesses because if they obtain information that is supposed to be maintained by the business as secure, these criminals could gain a great deal of control over your account.

Since the Bank of San Antonio does not implement, oversee or monitor the computer security infrastructure for bank client computers/networks, we are providing the information contained in this document to make you aware of these issues and provide a partial list of things that you can do to protect your money and information.

In one example of electronic attack, criminal hackers infiltrate your computers to install malware and viruses that capture the login, password and, in some cases, the dynamic security token number, information of a legitimate user. Criminal hackers can also launch what is called a "man-in-the-middle" or "man-in-the-browser" attack that captures online banking log-in information by asking a client to reenter log-in information, or to answer additional challenge questions. Capturing such information allows the thief to log in to the company's online banking system to **impersonate a legitimate company user**. The criminals can then transfer funds, typically by wire and/or ACH transfer, to accounts in other banks either inside of our outside of the U.S.

In another type of attack (one that is becoming more common) criminal hackers obtain all of the company's online banking information as discussed above, and then transfer the money by wire or ACH into the personal accounts of often-unwitting "electronic money mules." "Money mules" are people who have been previously recruited via Internet job posting sites for positions that include, among other seemingly legitimate job duties, processing payments to foreign entities out of their personal bank accounts. Criminals fraudulently transfer money from a company's account to the personal account of the electronic money mule, and then the electronic money mule is instructed to immediately withdraw the funds in cash and send the funds via Western Union, or MoneyGram or another international remittance company, and the funds are transferred out of the country just a few hours after the fraudulent transfer from the company.

Recommendations for Corporate/Commercial Clients:

The criminal hackers in these situations move very, very quickly and the stolen funds are typically not recovered. Losses of this type are most often the responsibility of the company, and not the Bank. The key to fighting this type of fraud and crime for a company is to take action to strengthen internal procedures and online banking procedures before becoming the victim of such an attack.

We strongly recommend that all of our commercial clients implement the following procedures and tools to help prevent criminals from accessing company accounts:

- Monitor your accounts frequently, and monitor and reconcile accounts daily as a best practice; immediately review wire, ACH or other commercial account transactions as quickly as possible after receipt.

- Implement a system of dual control and approval for ACH and wire transfers where dual approval is required prior to the transaction being initiated. Prior approval dual control means one employee originates/initiates the wire/ACH transaction or batch, and a second employee must authorize the wire/ACH transaction or batch prior to the Bank processing it. Dual control for initiation does not occur when one person can *initiate and approve* the transaction themselves, and a second employee receives the confirmation after the money has been sent.

- Never share User IDs, passwords, PIN numbers, dynamic tokens, etc., with anyone, and do not leave any such information or items in an area that is not locked/secured. Do not use the login or password for your financial institution on any other website or software.

- Obtain and install antivirus, anti-malware and anti-spyware software, and consider installation of a firewall. Make sure it is active and automatically updated by your vendor (or take necessary steps to keep it updated). NOTE: This measure will help protect against known viruses, malware and adware, but many viruses, malware and adware are undetectable by such data security programs, so this step is one of several security protection measures that should be followed.

- Limit or eliminate unnecessary web-surfing and/or email activity, including personal activity, on computers used for online banking. Many hacking attacks use social networking sites (such as FaceBook) to transmit computer viruses. Criminal hackers even use information on such social networking sites to "spear phish," or target specific individuals, such as a company's chief treasury management person or chief financial officer.

- You may also want to consider a dedicated computer for online banking that is never used for e-mail or general internet browsing/surfing.

- Educate all personnel on good cyber security practices, clearing the internet browser's cache before visiting the financial institution's website, and how to avoid having malware installed on a computer. For example, if a media player needs to be updated, go to the official media player website to install the update. Clicking on a fake update installation link could just mask a criminal hacker downloading malware onto your computer.

- Verify use of a secure session (“https://” and not “http://”), and avoid saving passwords to a computer.

- Never leave a computer unattended when using any online banking or financial services, and always lock your computer when you have logged off such sites and leave it unattended.

- Change, revise and re-visit those IT employees who have “keys to the kingdom” access for user approval, access rights and deleting/adding new users. While many attacks occur from outside hacking, insider hacking does occur, and dividing or rotating “keys to the kingdom” IT authority can cut down on opportunities for insider fraud.

- Never access your financial institution’s website for online banking (or any privileged or sensitive computer system) from a public computer at a hotel/motel, library or public wireless access point.

- Understand and carefully control the authorized users and permissions granted to any of your employees who are approved for online banking use and are issued unique User IDs, passwords (and tokens, if applicable).

- Immediately report any suspicious activity in your accounts to Bank personnel; there is a limited recovery window and a rapid response may prevent additional losses.

- Do not click on a link in any e-mail purported to be sent from Bank; Bank official e-mails will always instruct you to log in to online banking for updates, instructions, notifications, account statements, etc.

- Be suspicious of e-mails purporting to be from other financial institutions, federal, state or local government departments or agencies, or taxing authorities that request account information, account verification or banking access credentials such as User IDs, passwords, PIN codes and similar information. Opening attachments, or clicking on links in such suspicious e-mails, can also expose your computer to malicious code or malware that will be installed to your computer. Remember, legal process, subpoenas, and information from government agencies still generally comes as regular snail-mail.

- Bank’s online banking website is only scheduled for downtime for regular maintenance at certain times late in the evening/early morning, and never during prime business hours. If you log into online banking and receive a message such as “please wait for website update, which will take approximately 15 – 20 minutes,” immediately contact Bank personnel to determine if it is a legitimate delay in online banking services caused by the Bank.

- Consider implementation of ACH debit blocks, wire/ACH per transaction dollar limits and other methods to mitigate potential risk exposure.

If you suspect someone is attempting to gain access, or has already gained access, to your Online Banking information, immediately stop using any computers that may be affected and contact Bank personnel at 210-807-5555 to request help in preventing further loss and to aid in the possible recovery of funds fraudulently transferred.

In addition to the steps listed above, Bank also offers a variety of services that can help you protect your accounts from check and ACH fraud. For more information about these products and services, please contact your banker or a Bank Treasury Management professional.

Recommendations for Consumer Clients:

As an added caution to our consumer clients, we want to address a growing problem of unwitting individuals being recruited via online job sites and similar online job offers, into situations where they become "electronic money mules," instead of obtaining gainful employment. According to the Federal Deposit Insurance Corporation, "electronic money mule" activity is essentially electronic money laundering addressed under the Bank Secrecy Act and anti-money laundering regulations. Many corporate account take over and fraud schemes rely on electronic money mules receiving stolen money into their personal accounts and transmitting the stolen funds outside the U.S. Once recruited, an electronic money mule is instructed to use their existing personal account, or to open up another personal bank account.

Any employment position that requires use of a personal account for business purposes should be highly suspect, and you should not respond to such offers for employment as a mystery shopper, payment processor, etc., where you are required to use your personal account for someone else's business purposes. No legitimate business will attempt to move business funds through anyone's personal account, and you should educate yourself on these issues. If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Secret Service to let them know.

DISCLAIMER: The industry information included in this document is provided for general purposes only and Bank of San Antonio does not provide any express or implied warranty, guarantee or promise concerning the content, completeness, accuracy or value of the information. All persons or entities should confirm the accuracy as it applies to their specific business or system. This alert is provided as information only, and Bank of San Antonio will have no liability to a client, or any other person or entity, for any direct, indirect, incidental, special or consequential damages arising out of the information contained in this alert.