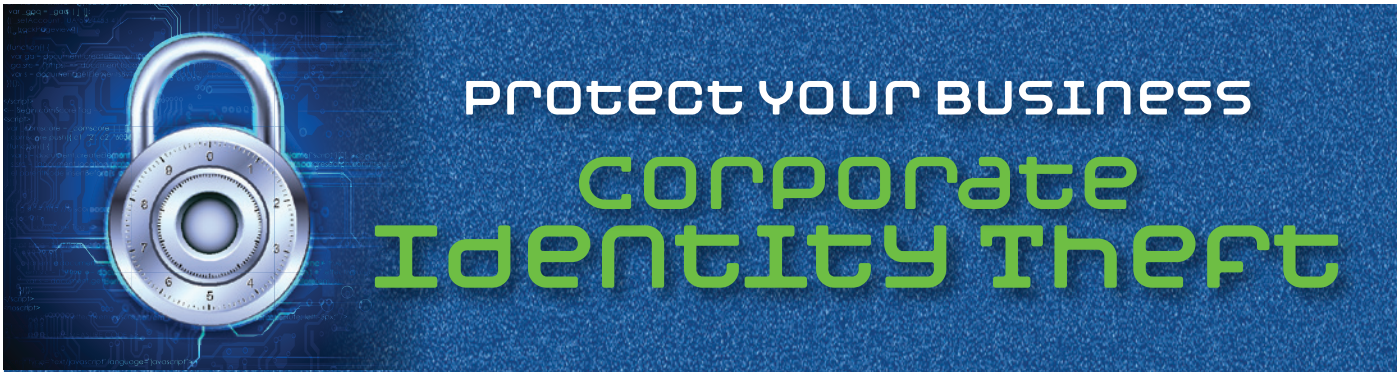

Protect Your Business

Corporate Identity Theft

First State Bank of Bedias would like to make you aware of a growing threat to your business, Corporate Identity Theft (Corporate Account Takeover).

Corporate Account Takeover *is the business equivalent of personal identity theft. It is a form of identity theft where a business' online credentials are stolen by malware (software that hackers use to control your computer) that infects computer devises but not limited to workstations and laptops. Criminal entities then have the opportunity to initiate fraudulent banking activity.*

A business can become infected with malware *via infected documents attached to an email or a link contained within an email that connects to an infected Web site. In addition, malware can be downloaded to users' workstations and laptops by visiting legitimate Web sites - especially social networking sites - and clicking on the documents, videos or photos posted there. This malware can also spread across a business' internal network.*

Corporate Account Takeovers have continued to grow and evolve in their sophistication. *Although First State Bank of Bedias uses technologies such as multi-factor authentication and encryption, there are additional controls that can be instituted to further reduce the risk of Corporate Account Takeover and fraud.*

- *Reconcile your banking transactions on a daily basis.*
- *Initiate ACH and wire transfer payments under dual control, with a transaction originator and separate transaction authorizer or approver.*
- *If possible, carry out all online banking activities from a stand-alone, up to date (with all operating systems, virus protection, etc) and completely locked down computer system from which email and Web browsing are not possible.*
- *Be suspicious of emails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack your computer.*
- *Install a dedicated, actively managed firewall, especially if the business has a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.*
- *Create strong passwords with at least 10 characters that include a combination of mixed case letters, numbers and special characters. Prohibit the use of "shared" usernames and passwords for online banking systems.*
- *Use a different password for each Web site that is accessed. Change the password a few times each year.*
- *Never share username and password information for Online Services with third-party providers.*
- *Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.*

Educate employees on good cyber security practices *to include how to avoid having malware installed on the business computer.*
Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
Ensure virus protection and security software are updated regularly.
Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
Consider installing spyware detection programs.

- *Clear the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.*
- *Verify use of a secure session (https:// not http://) in the browser for all online financial transactions, including online banking.*
- *Avoid using automatic login features that save usernames and passwords for online banking.*
- *Never leave a computer unattended while using any online banking or investing service.*
- *Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.*
- *Properly log out of each online banking session and close all browser windows. Simply closing the active window may not be enough.*
- *When finished with the computer, turn it off or disconnect it from the Internet.*
- *Consider utilizing a security expert to test the network or run security software that will aid you in identifying known vulnerabilities.*

For additional information and resources on Corporate Account Takeover and other save business practices, visit First State Bank of Bedias' Education Center and view the Business Education tab.

Be sure to report any suspicious activity or unauthorized transactions on your account, as soon as you are aware. You may report the activity in person at any of our First State Bank of Bedias branch locations or by calling immediately at 936-395-2141 or 979-589-2407.

FIRST STATE BANK *of* BEDIAS
★ Since 1907 ★

Bedias: 22201 Hwy. 90 North • P.O. Box 99 • Bedias, Texas 77831 • 936.395.2141
Kurten Banking Center: P.O. Box 168 • Kurten, Texas 77862 • 979.589.2407
MEMBER FDIC • bediasbank.com