Metairie Bank

WHAT YOU NEED TO KNOW ABOUT CORPORATE ACCOUNT Takeover

WHAT IS CORPORATE ACCOUNT TAKEOVER?

• **CORPORATE IDENTITY THEFT.** Simply put, corporate account takeover is the business equivalent of personal identity theft. Hackers, backed by professional criminal organizations, are targeting small and medium businesses to obtain access to their web banking credentials or remove control of their computers. These hackers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through mules that quickly redirect the monies overseas into backer's accounts. A computer can be compromised very easily by visiting an infected website or by simply opening an email. There has been a steady increase in account takeovers since 2009 resulting in billions of dollars of damage.

SECURITY BEST PRACTICES

• **A SOLID FOUNDATION TO BUILD ON.** When it comes to protecting sensitive financial information from hackers, there's no substitute for good old-fashioned knowledge. As a business owner, you should have a level of understanding about how to secure your computers that allows you to take proactive steps and avoid, or at least minimize most threats. Experts advise following best practices including using a dedicated computer, keeping patches and anti-virus up to date, installing a host based firewall, verifying all transactions before approving and reviewing bank transactions daily. These best practices should be the minimum security baseline for every company's online banking transactions.

If you believe your Metairie Bank account has been compromised contact us immediately at 504-834-6330.

We connect with you.

CALL, CLICK OR COME BY.

SOUTHSHORE 504.834.6330 | NORTHSHORE 985.674.2255

STEPS FOR BETTER SECURITY

- Use a **DEDICATED COMPUTER** for financial transactional activity. Do not use this computer for general web browsing and email.
- Apply **OPERATING SYSTEM AND APPLICATION UPDATES** regularly (patches).
- Ensure that **ANTI-VIRUS/SPYWARE SOFTWARE** is installed, functional and is updated with the most current version.
- Have host-based **FIREWALL** software installed on computers.
- Use the **LATEST VERSION OF INTERNET BROWSERS,** such as Explorer, Firefox or Google Chrome and keep patch up to date.
- Activate a **"POP-UP" BLOCKER** on internet browsers to prevent intrusions.
- **TURN OFF YOUR COMPUTER** when not in use.
- **DO NOT BATCH APPROVE TRANSACTIONS;** be sure to review and approve each one individually.
- Review your **CREDIT REPORT/BANKING TRANSACTIONS** regularly.
- **CONTACT YOUR INFORMATION TECHNOLOGY PROVIDER** to determine the best way to safeguard the security of your computers and networks.

WARNING SIGNS

Warning signs visible to a business or consumer customer that their system/network may have been compromised include:

- Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money);
- Dramatic loss of computer speed;
- Changes in the way things appear on the screen;
- Computer locks up so the user is unable to perform any functions;
- Unexpected rebooting or restarting of the computer;
- Unexpected request for a one time password (or token) in the middle of an online session;
- Unusual pop-up messages, especially a message in the middle of a session that says that the connection to the bank system is not working (system unavailable, down for maintenance, etc.);
- New or unexpected toolbars and/or icons; and
- Inability to shut down or restart the computer.