Bank of Tennessee

Carter County Bank

Mountain Community Bank

CARTER COUNTY BANK AND MOUNTAIN COMMUNITY BANK ARE DIVISIONS OF BANK OF TENNESSEE MEMBER FDIC

Protect Your Business from Corporate Account Takeover

Corporate Account Takeover is a form of business identity theft where the online credentials for the business, municipality or non-profit are stolen by malware. Hackers backed by professional criminal organizations, are targeting businesses and other entities to obtain access to their web banking credentials or to remotely control their computers. These hackers will then drain the deposit and credit lines of the compromised bank accounts. They funnel the funds through "money mules" - unwitting, often innocent accomplices who facilitate the quick redirect of the monies overseas into the hackers' accounts.

Can It Really Happen to My Business?

Banks follow specific rules for electronic transactions issued by the Federal Reserve Board known as Regulation E. These protections provided under Reg E are only extended to consumers. Businesses, Non-Profit organizations and other entities have limited protection against fraudulent electronic transactions such as those processed through online banking.

Is My Business Protected?

Banks follow specific rules for electronic transactions issued by the Federal Reserve Board known as Regulation E. These protections provided under Reg E are only extended to consumers. Businesses, Non-Profit organizations and other entities have limited protection against fraudulent electronic transactions such as those processed through online banking.

How Do Criminals Get Access to My Account?

Two of the most common techniques hackers use are "phishing" and "pharming".

1) **Phishing** - (pronounced "fishing") is a prolific scam wherein a fraudster or scam artist sends an e-mail purporting to be from a financial institution or other organization. The message includes a call to action by the recipient to click on an imbedded link due to "security concerns", "too many attempted log-ins", an urgent need to "authorize attempted transactions", or other such reasons, the recipient must confirm their personal and account information immediately to avoid some negative consequence - such as imminent account closure. The e-mails look and sound official, and often contain graphics stolen from the company or organization from which the message claims to originate. The e-mail generally contains a link to a spoofed website that contains stolen graphics, logos, and information taken from the legitimate organization's website in order to give the appearance of being the actual site. If you attempt to log in, you have just provided the

criminals your log-in credentials to the real website. The website addresses used in these scams are frequently very close to the real organization's website address, though they often contain an additional series of letters or numbers such as *www.yourbank3qm.com* or *www.yourbankcustomerservice42.com*.

In other cases, it may be deceptively established as a sub-domain of another website address, such as www.yourbankname.vwxyz.com. Think before you click. Web addresses and links can also be easily masked in phishing emails, wherein the address link that is visibly displayed to the reader appears to be legitimate, but in actuality, it is merely hiding or masking the real link to the bogus site. This is one reason why you should not blindly click on links in emails sent to you by unknown persons.

2) **Pharming** - (Also Domain Spoofing and DNS Poisoning) is a term derived from "phishing", is a scam wherein a cyber-criminal exploits vulnerability in a user's computer HOSTS file or "poisons" an Internet Service Provider's Domain Name Server (DNS) software to trick a user's computer into visiting a seemingly legitimate, yet entirely bogus website. The intent is to cause the user to believe that he or she is visiting the legitimate web site and then attempt to log in or unknowingly provide personal and confidential information that can then be used by the criminal to commit fraud or identity theft. The spoofed website typically contains stolen graphics, logos, and information taken from the legitimate organization's website in order to give the appearance, at least on the surface, of being the actual site. Pharming sites are usually not very deep, often consisting only of two to three pages. If visitors attempt to navigate through the site they will find numerous broken links, site errors, and many non-existent pages. The site only needs to appear legitimate just long enough to convince the visitor to attempt to log in or provide information.

Best Practices for Your Computer Network Administration

- 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.
- Ensure that anti-virus/spyware software is installed, functional and is updated with the most current version.
- Implement multi-layered system security technology. Anti-virus software, alone, will not protect a business from most threats. Layering security software constructs a multi-level barrier between business' networks and criminals attempting to access such networks.
- Have host-based firewall software installed on computers.
- Use latest version of Internet browsers, such as Explorer, Firefox or Google Chrome and keep patches up to date.
- Activate a "pop-up" blocker on Internet browsers to prevent intrusions.
- Turn off your computer when not in use.
- Use strange character combinations for passwords and change them frequently on both the computer and online banking.

Best Practices in Managing Your Business' Financial Transactions

• Do not batch approve transactions; be sure to review and approve each one individually.
• Monitor and report suspicious activity on your account.
• Set up account alerts through online banking to notify you when unusual conditions on your account, such as a minimum balance level is reached or a transaction over a specified amount is performed.
• Set user limits for online banking transactions.
• Initiate payments under dual control, with assigned responsibility for transaction origination and authorization.
• Take advantage of appropriate account services like positive pay, debit blocks, call backs, etc.
• Use multi-channel authentication for business accounts that are permitted to initiate funds transfers.
• Perform a risk assessment on your business on an annual basis. Bank of Tennessee has a free Business Technology Risk Assessment we will provide to you at no charge.
• Educate all computer users about cybercrimes so everyone understands that even one infected computer can lead to an account takeover.

How and When We Will Contact You

Bank of Tennessee will never ask you for personal information, including your online banking credentials through email.

If You Suspect Fraudulent Activity

Should you notice suspicious activity on your account or experience security-related events, contact us immediately through our Customer Care Center at 866.378.9500 or customercare@bankoftennessee.com.