Avoiding Corporate Account Takeover

Wrentham Cooperative Bank takes the safety and security of your financial information very seriously. However, we need your cooperation and participation in these efforts to keep your information and assets safe from the cyber-criminals that are looking for new businesses to target every day. These criminals know that banks invest time and money in building systems that will keep them out. Instead, they are counting on you, the business owner to be the weak link.
In order to help you avoid becoming the next victim, we have put together this information. If you read and follow these guidelines, you will help protect your assets and your business.

To understand how to avoid corporate account takeover (CATO), it is important to have a clear understanding about what is.

Definition:

Corporate Account Takeover is a form of corporate identity theft where a business' online credentials (User name, password, etc.) are stolen by computer malware. Criminals can then initiate fraudulent banking activity. Cyber-criminals are targeting small to medium sized businesses to obtain access to their online banking credentials. The perpetrators drain the deposits and credit lines of the compromised business bank accounts.

A computer can be compromised very easily by visiting an infected website or by opening an email containing an infected link or attachment.

Security Steps Every Business Should Consider When Conducting Online Banking

1. Use a dedicated computer for financial transaction activity. **Do not** use this computer for general browsing and/or email. This will significantly reduce the risk of your computer getting infected and your financial records being compromised.
2. Keep your systems up to date and protected by applying operating system and application updates regularly.
3. Ensure that you install the most updated versions of anti-virus/spyware security software and have firewall software installed on the dedicated computer.
4. Regularly run anti-virus scanning on your computer.
5. Use the latest version of Internet browsers, such as Safari, Internet Explorer, Firefox, or Google Chrome and keep patches (security updates) current.
6. Activate a "pop-up" blocker on browsers to prevent "drive-by" infections.
7. Do not store passwords in your browser.
8. Do not share user ID's and passwords among your staff.
9. Turn the computer you use for online banking off when not in use.
10. Review your banking transactions regularly.

11. Talk with your IT provider to determine the best way to safeguard your computers and network.

Important Information About Banking Regulation "E"

Protections against losses due to fraud under banking regulation E ("Reg E") are very different for businesses than they are for consumers. A non-consumer using Internet banking and/or Bill Pay is **not protected under Regulation E**. In light of this, special consideration should be made by the business customer to review the controls they have in place to ensure that they are commensurate with the risk level that they are willing to accept.

If you believe your Wrentham Cooperative Bank account or online banking access has been compromised, contact Wrentham Cooperative Bank immediately at 508-384-6101.

Wrentham Cooperative Bank will never contact you to ask for your account number, PIN, Password or other personal information via email, telephone or provide links within an email to update information. If you receive a request for your personal information, or you suspect you have inadvertently provided personal information to a questionable person, call us at 508-384-6101.