What is Corporate Account Takeover?

Corporate Account Takeover is a fast-growing crime where thieves use computer '*malware*' to steal online banking credentials or hijack login sessions and fraudulently transfer funds from the victim's accounts.

Domestic and International Wire, ACH and Bill Pay transfers are the most popular methods for transferring funds.

Malware, short for *malicious software*, are programs designed to infiltrate a computer or network undetected and provide confidential information to the thieves such as access IDs, passwords, internet browsing activity and other personal and confidential information. Key logging and screen capture software allow the criminals to gather the necessary data.

Malware includes computer viruses, spyware and other malicious software that is introduced into a computer system by various methods, including e-mail attachments, website links, internet ads, P2P networking sites, social networking sites, software downloads and USB "thumb" drives.

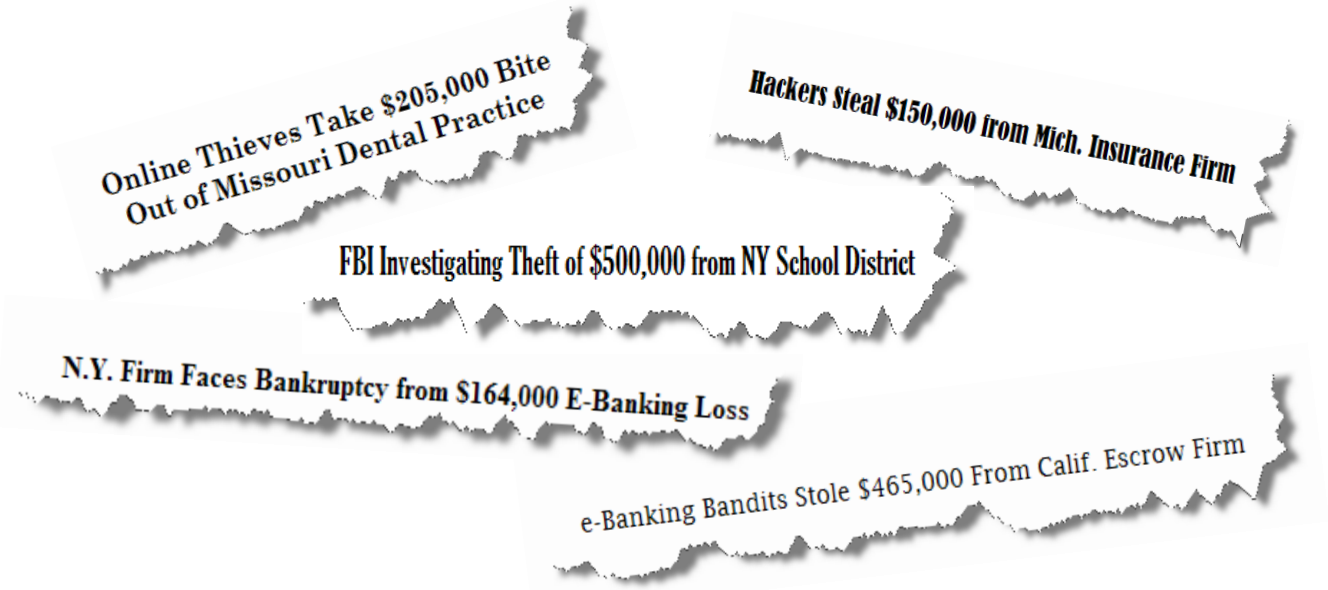

***Figure 1**. Information "ripped from the headlines" shows recent losses due to cyber crime activity.*

How Does it Happen?

Cyber criminals, once armed with confidential information gathered from malware installed on the victim's computer, can now hijack or begin an online banking session from their own PC or the victim's PC – sometimes at the same time that the user is conducting his/her online banking transactions. Often, the user is prompted to enter passwords and other security information during the online banking session even though the transaction being initiated by the user doesn't warrant authentication. *For example, the user is reviewing recent account deposit history and is suddenly prompted for her token-generated one-time password typically required for high-risk transactions, such as wire transfers.*

These events often coincide with unusual website behavior (such as long delays, unfamiliar screens or outage notifications) or even unsolicited telephone calls from someone purporting to be from the bank.

How Do I Protect Myself and My Company?

The most effective way to protect against cyber fraud is to keep yourself and your staff updated with the most recent fraud trends and keep your computer updated with the most recent software/hardware protections available. This includes:

Computer/Network

- Password protect your PC.
- Use a computer designated only for online banking activity (no e-mail or other internet use).
- Install, update and enable Internet Security Software, including anti-virus, anti-spyware and other malware detection.
- Perform browser and operating system updates regularly.
- Install/configure firewalls and routers to prevent unauthorized access to your computer or network.
- If no one in the company has sufficient time, resources or training, hire an IT professional to install, configure and maintain your computers, network, firewall and internet security software.

Behavior

- Be wary of unsolicited emails or pop-up messages, and do not open attachments or click hyperlinks.
- Do not provide sensitive information to unknown parties over the phone, through e-mail or on an unfamiliar website, including credit/debit card numbers, passwords or other personal data.
- Watch for unexpected activity such as being prompted for a token generated one-time password while simply viewing accounts online.
- Note changes to PC performance (e.g. unexplained slow-downs), unusual login delays and new or unusual icons or toolbars.
- Do not use public internet access points (e.g. internet cafes, public Wi-Fi hotspots, etc.) to access online banking or other secure sites.
- Stay informed and train office staff about internet fraud scams.

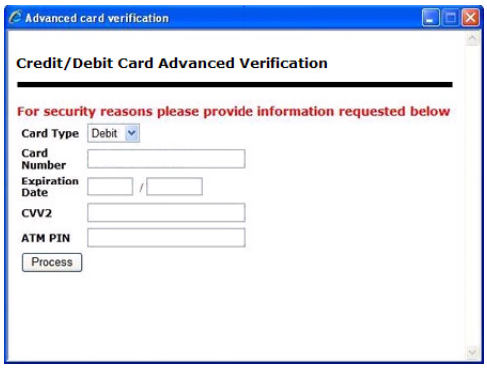

***Figure 2**. Phony website prompting for card information.*

Online Banking & Administration

- Review account activity daily.
- Reconcile accounts timely; utilize transaction exports to populate financial management software, such as QuickBooks©.
- Require dual-authorization for high-risk transactions (e.g. wire transfers, ACH transfers and online bill pay).
- Establish client or employee transfer limits.
- Update and regularly review employee access permissions.
- Register computers during login process.

What if I Believe That I am a Victim of Internet Fraud?

CONTACT THE BANK IMMEDIATELY if you believe that your online banking profile has been compromised or you may be a victim of internet fraud or account takeover.

Customer Service (toll-free): (866) 224-1379 **Online Banking Support: (973) 948-9520**