PROTECTING YOUR BUSINESS:

CyberCrime Edition

WHAT IS A CORPORATE ACCOUNT TAKEOVER?

Well-organized cybercrime syndicates are targeting small and medium size business, municipalities, non-profits and school districts across the country. Cyber criminals use **mal**icious soft**ware** (known as **malware**) in order to steal a business' online banking credentials or take over web sessions. They then attempt to steal thousands, even hundreds of thousands of dollars, by creating fraudulent ACH or wire transfers. This crime is known as Corporate Account Takeover.

It is very important to recognize that Corporate Account Takeover attacks are not aimed at financial institutions; they target accountholders, specifically the computers and Internet connections that are used to access online bank accounts. It is the accountholder's responsibility to secure workstations, network connections and account credentials. Federal Regulation E does not apply to commercial accounts and financial institutions are not required to reimburse losses under certain circumstances.

Anatomy of a **Corporate Account Takeover**

1 TARGET VICTIMS

Criminals target victims by way of phishing, or social engineering techniques. Their goal is to deliver malware to the workstation used for Internet Banking.

2 INSTALL MALWARE

The victims unknowingly install malware on their computers, which is programmed to steal online banking credentials by recording keystrokes or copying what is on the screen, and connect back to a "command and control" center to listen for and execute instructions.

3 ONLINE BANKING

The victims visit their online banking website and logon per the standard process. This action activates the malware.

4 COLLECT & TRANSMIT DATA

The malware collects and transmits data to the criminals through a back door connection.

5 INITIATE FUND TRANSFER(S)

The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.

...and how to prevent it.

1 USE A RESTRICTED WORK STATION

The workstation used for online banking, specifically cash management (ACH and wire) transactions, should not be used for email, social networking, web browsing, game playing, shopping, watching movies or downloading music. These are all malware delivery channels.

2 BE EMAIL AWARE

Don't respond to or open attachments or click on links in unsolicited emails. Never respond to unsolicited requests for information.

3 MAINTAIN REAL-TIME ANTIVIRUS AND MALWARE DETECTION & SECURITY UPDATES

Install and maintain real-time antivirus and malware detection. Allow for automatic updates and scheduled scans. Install operating system and application security updates as soon as they become available.

4 SECURE YOUR INTERNET CONNECTION

Install routers and firewalls to prevent unauthorized access to your computer or network. Always change the default administrator password.

5 DO NOT USE PUBLIC Wi-Fi FOR ONLINE BANKING

Do not use public internet access points, e.g. internet cafes or public Wi-Fi hotspots (airports, etc.), to access accounts or personal information.

6 LEARN MORE ABOUT ONLINE BANKING CONTROLS

Ask your banker about multifactor authentication, dual controls, alerts, daily and weekly limits and transaction verification. Recognize that sometimes you may need to sacrifice a little bit of convenience for a whole lot of security.

7 DON'T IGNORE WARNING SIGNS

Watch for new toolbars and/or icons, a request for a one-time password (or token) in the middle of an online banking session, pop-up messages requesting information, or an online banking session being suspended or timing out.

Monitor and reconcile your account.
Reviewing accounts regularly helps enable quick detection of unauthorized activity, and allows your business and your financial institution to take action to prevent or minimize losses.

If you suspect a compromise...
Immediately disconnect your workstation from the internet, cease all online banking activity on all workstations and call your financial institution.

Protect, Detect and Respond

Norway Savings Bank

Protect

Online Account Review

- Review your account activity using the online transaction history to review for unauthorized activity. ***We recommend reviewing your account on a daily basis. You should also be reviewing your statements.***

Internal Online Banking Controls

- Always keep your Internet Banking credentials confidential. Your personal credentials are something only you should know and should not be shared with anyone. If you suspect it has been compromised, change it immediately and contact the bank
- Safeguard your security token (if you have been issued one).
- Log out of online banking when done.
- Consider conducting a risk assessment of your online banking activities on a periodic basis. This risk assessment should review your controls in place as well as identify changes that may have reduced the desired level of security control in your environment. Online business transactions that involve ACH origination and frequent wire transfers have a higher risk. Dual control, token authentication, segregation of duties, and authorization call backs are all additional protections that can afford added layers of security.
- View our "Corporate Account Takeover" online video training found on our website at norwaysavingsbank.com.

Detect

- Watch for red flags such as
  - unexpected password resets, unknown transactions or suspected user credential compromise.
  - suspected embezzlement or other security incident that might compromise your Company's computer or network security.
- Never respond to unsolicited requests for information.
  - Norway Savings Bank will **never** contact you and request your online banking credentials. If you receive a request for this information either over the phone or online, **DO NOT** provide it.

Respond

- **Should you suspect any suspicious activity, please notify the Bank immediately at (888) 725-2207.**
- Immediately discontinue using any computer equipment for Internet banking activity that is suspected of being infected with any type of malicious software or viruses.
- Seek the help of an IT professional in order to restore the security of the equipment before resuming Internet banking activities on it.
- Continue to monitor and immediately report any transactions made to your accounts that appear to be questionable