CORPORATE ACCOUNT TAKEOVER:

AMERICAN MOMENTUM BANK®

HOW TO PROTECT YOUR BUSINESS FROM CORPORATE ACCOUNT TAKEOVER

What is Corporate Account Takeover?

Corporate Account Takeover is a form of cyber fraud that illegally accesses business accounts electronically resulting in monetary loss due to fraudulent transfers.

How it's Done:

Cyber criminals gain access to business accounts through technology based methods. This is done when victims are tricked into giving access or providing confidential or business account information to cyber criminals online.

Once a business owner or employee clicks on a fraudulent email or website link, the malware infects the victim's computer and allows the criminal to see and track information that ultimately leads to compromised banking credentials. With compromised banking credentials, the cyber criminal gains access to business accounts and initiates fraudulent account transfers. Some examples of activities that can lead to Corporate Account Takeover include**:**

- Opening an email and clicking a fraudulent link.
- Visiting a compromised website that installs malware on your computer.
- Accepting a fake friend request on social media networking sites and providing personal information.

How to Protect Yourself:

As a business owner or employee, there are some actions that you can take to help minimize the potential of being a victim of Corporate Account Takeover:

- Educate all employees on this type of fraud scheme.
- Enhance the security of your computer and networks to protect against this fraud.
- Enhance the security of your corporate banking processes and protocols.
- Monitor and reconcile accounts at least once a day.
- Run regular virus and malware scans of your computer's hard drive.

BUSINESS EMAIL COMPROMISE:

AMERICAN MOMENTUM BANK®

HOW TO PROTECT YOUR BUSINESS

What is Business Email Compromise (BEC)? A sophisticated scam that utilizes legitimate email accounts to steal money or personal information from a business. These scams target businesses that use wire transfers, foreign suppliers and other invoice transactions.

Examples of Business Email Compromise:

- **Business Executive Scam:** Scammers will use your email address to contact an employee responsible for your company's finances, requesting a large wire transfer into their fake accounts. Fraudsters will usually indicate that the transfer must be done urgently and quietly. Since most businesses utilize email as their main form of communication between employees and departments, this type of BEC is almost always detected after the transfer has been made.
- **Supplier Swindle Scam:** The second method targets your company's foreign suppliers or overseas vendors, again, hoping to authorize wire transfers to a fake account. Criminals can hack into your supplier's email account and request a wire transfer to a "new" account, disclosing that the supplier's location overseas has moved or changed.
- **Bogus Invoice Scam:** The third method targets your customers or third-party vendors, hoping to collect their money through false invoice requests. Fraudsters can hack into your employees' emails and send out urgent invoices, similar to the method used with overseas suppliers.
- **Personal Data Scam:** Unlike the first three methods, this final method focuses on stealing your employees' personal information. Fraudsters target your human resources' email accounts to obtain personally identifiable information (PII), specifically W-2 information. Emails are sent from your HR representative's hacked email account to other employees, asking to either provide or verify their sensitive information.

How To Protect Yourself:

Below are tips to help protect you and your business from being a victim of Business Email Compromise:

- **Education Training:** Educate your staff about the common red flags of BEC scams. Encourage them to investigate emails regarding wire transfer, invoice, or sensitive information.
- **Personal Information Security:** As always, emphasize the importance of protecting personally identifiable information, even in the workplace. Instruct employees to always safeguard their sensitive information, and encourage them to deliver W-2 and tax form information to your human resources in person.
- **Protocol:** Put in place and adhere to a strict protocol and policy regarding wire transfer or invoice requests. Following a consistent process will make it easier for employees to spot suspicious behavior.
- **Open Communication**: Encourage face-to-face or phone conversations between departments in situations where wire transfers or invoice requests are asked to be done urgently or quietly.