Corporate Account Security

Growing Threats To Your Business – Are You Aware?

Corporate Identity Theft (Corporate Account Takeover) is the business equivalent of personal identity theft and occurs when criminal hackers use software, often referred to as malware, to control your computer devices and steal your online business credentials. The criminals then use your online business credentials to initiate fraudulent banking activity.

Your devices can become infected with malware when you attempt to open an infected document attached to an email – or an infected website link within an email. Malware can also be downloaded to a device when you visit a legitimate site, especially a social networking site, and attempt to open a document, video, or photo posted there. Once the malware infects one device, it often has the ability to quickly and efficiently identify and infect other devices within an internal business network – often without detection.

What You Can Do To Protect Yourself and Your Company

Although Endeavor Bank uses technologies such as two-factor authentication and encryption methods that help mitigate the risk of fraudulent banking activity, these technologies cannot protect against malware that attack your devices. There are additional controls that you should consider implementing to further mitigate the risk of Corporate Account Takeover and fraud.

- Never provide your account information or password over the phone or email. We will **never** ask you to enter personal or account information via email or to download an attachment from email, nor ask you for your password or other security credentials via email or phone.
- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Employ best practices to secure computer systems. If possible, carry out all online banking activities from a stand-alone, hardened, and completely locked-down computer system from which email and web browsing is not possible. When finished, turn it off or disconnect it from the internet.
- Be suspicious of emails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or

banking access credentials such as usernames, passwords, token codes, and similar information. Opening file attachments or web links in suspicious emails could expose your entire network to malware.
- Install a dedicated, actively managed firewall, especially if your business has a dedicated connection to the Internet. A firewall limits the potential for unauthorized access to a network and computers.
- Create strong passwords with at least 10 characters that include a combination of mixed case letters, numbers, and special characters. Use a unique password for each financial institution site that is accessed and change that password regularly. Avoid using dictionary words in your passwords.
- Educate employees on good cybersecurity practices, including how to avoid malware infections on business computers.
- Never access bank, brokerage, or other financial services information using public Wi-Fi at airports, hotels, cafes, libraries, etc. Unauthorized software may have been installed to trap account numbers and sign-on information, leaving you vulnerable to possible fraud.
- Install commercial antivirus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats when compared to an industry-standard product. Ensure computers are patched regularly, particularly operating system, web browsers, and key applications with security patches. It may be possible to sign up for automatic updates for operating systems, browsers, and many applications.

What We Do To Help Mitigate Your Risk

POSITIVE PAY
Endeavor Bank offers this important product that helps you detect and prevent check fraud.

- Save time by using this automated online tool to review and decision any check that doesn’t match your Check Issues list.
- Conveniently upload your Check Issue information through our secure online portal.
- Gain greater control of your cash flow by proactively monitoring all checks that clear your business accounts.

OUT OF BAND AUTHENTICATION
Out of Band provides greater protection from fraudulent access to user account information.

- First-time users logging into their Digital Banking Account will be prompted to confirm their identity through the Digital Banking Advanced Login Authentication solution, also known as Out of Band.
- Allows users to authenticate using their username and two additional methods; their password and a one-time security code.

DUAL CONTROL ENVIRONMENT
Endeavor Bank strongly recommends that our clients operate in a Dual Control environment when initiating ACH and Wire Transfers, as well as Self-Administration tasks. Business Digital Banking provides our clients with the ability to entitle users with specific privileges; such as Initiators and Approvers.

SUSPICIOUS ACTIVITY
Report unauthorized transactions on your account immediately. You may report the activity in person or at our branch location or by calling **619-329-6565**. If you are a victim of internet fraud you should file a complaint at the Internet Crime Complaint Center by visiting www.ic3.gov, a partnership between the National White Collar Crime Center and the FBI.

IT'S ABOUT YOU
We hope you've found this informative and helpful. All of us at Endeavor Bank remain devoted to safeguarding and ensuring your security while banking with us. We also welcome the opportunity to talk to you about meeting and exceeding any and all business and personal banking needs you may have.