Business Online Cash Manager

Security Guide

MidWestOne Bank.

102 South Clinton Street
Iowa City, IA 52240
1-800-247-4418

Version 1.1

[This page intentionally left blank.]

Contents

[This page intentionally left blank.]

Introduction

PURPOSE

The purpose of the guide is to make you aware of the risks your business is exposed to when using a financial institution's online banking service. Small to medium sized businesses, non-profits, and municipalities have become popular targets among cybercriminals. This guide provides important information regarding the tactics these cybercriminals use and how you can protect your business. Please be advised that this guide does not include all potential security controls. Implementing the controls provided in this guide will not guarantee the protection of your online accounts; however, they will go a long way in preventing fraud from occurring.

CORPORATE ACCOUNT TAKEOVER ATTACKS

Corporate Account Takeovers are attacks carried out my cybercriminals that either obtain the login credentials or hijack the secure online sessions of legitimate users through the use of malicious software. The criminals then initiate wire and/or ACH transactions through the victim's corporate online banking account. These attacks typically begin with the introduction of malware. These malicious programs, such as spyware and viruses, can be spread between computers by e-mail, infected websites, and other means.

Since business accounts typically maintain higher cash balances, or have access to additional means of credit, than consumer accounts, Corporate Account Takeover schemes can net cybercriminals substantial profits. This, along with that fact that these cybercriminals often face a minimal chance of prosecution by their home country's government; means they are relentless in their efforts. They trick individual account holders, or money mules, into transferring funds stolen from compromised businesses to accounts held overseas. Money can vanish in as little as one business day. Corporate Account Takeover attacks cost businesses and financial institutions millions of dollars every year. If you have access to originate wire, ACH, or bill pay transactions through your online banking account with MidWest*One*, it is essential that you consider implementing the controls outlined in this guide.

Although our Business Online Cash Manager service offers substantial benefits to your business; having the appropriate security controls in place is critically important. Please feel free to contact us if you have any questions regarding this information.

Thank you for banking with MidWest*One* Bank!

Top Security Tips

ASSESS YOUR RISKS

Before you can begin to secure your electronic assets, assess what risks you face based on what data you store and to what degree a system compromise would impact your business. In today's world, a computer system compromise would drastically affect most businesses. Identify the risks and proceed to implement the appropriate controls. Conduct these risk assessments periodically. Also, don't forget to protect your own customer data. If you are unsure about what precautions need to be taken, consider seeking the help of an IT security professional. Additional tips from various trade organizations can be found on page 9 of this guide.

UTILIZE ANTI-VIRUS & ANTI-MALWARE SOFTWARE

All computers on your business network should have anti-virus and anti-spyware programs installed. These programs detect and respond to threats that may reach the computer through an e-mail attachment or website. Malicious software, such a computer viruses or spyware, can be used to collect confidential information or even to take control of the entire computer. Consider purchasing a business security suite from a security software developer.

FIREWALL

A firewall prevents unauthorized access to your business computer system by restricting allowable communication. Most operating systems have a built-in firewall feature, but you still need to verify that a firewall is indeed present and that it is turned on. Firewall programs are also readily available from security software providers and are often included when a business security suite is purchased.

EDUCATE YOUR EMPLOYEES

Educating your employees, especially those with access to online banking, is one of the most important precautions to take. Employees must be made aware of the risks associated with online banking and need to know they are the first line of defense. Topics to educate employees about include:

- **E-mail is not a secure communication channel**
  - **E-mail addresses can be spoofed to appear from a known person**
- Acceptable use of work computers
- Proper IT security procedures
- Signs of a malware infection
- Identifying fraudulent e-mails
- **General information regarding Social Engineering threats**

UPDATE & PATCH SOFTWARE

The security software protecting your business will be ineffective if it is not routinely updated. Any program your employees use needs to be updated with the latest patches to protect against new threats. Make this a priority for your business.

IMPLEMENT DUAL CONTROL

Our business internet banking service offers a dual control feature. Under dual control, all transaction requests must be submitted by one user and approved by another user before processing. This security control can greatly reduce the likelihood of fraud if the transaction is initiated and approved on two different computers. We highly recommend that you consider this feature and please contact us if you think it is right for your business.

STAND-ALONE MACHINE OR LIMITED BROWSING

If your employees have access to surf the internet on their work computer, they are exposing your computer system to additional risk. Consider limiting browsing privileges or establishing a machine that will strictly be used for online banking. Ensuring that computer is only used for online banking will drastically lower the chances of it becoming compromised via an infected e-mail or website. Only the stand-alone computer, no other device, should be used for accessing online banking.

ADDITIONAL TIPS

- Monitor account activity, check at least once daily
- Discourage password sharing between employees
- Enforce a strong password policy on all network computers
- Do not send confidential information via e-mail
- Shut down or disconnect computers from the internet when not in use
- Avoid unsecure Wi-Fi
- Back up and encrypt your data
- Limit administrative access

The Threat of Social Engineering

The first step of a Corporate Account Takeover attack typically includes some kind of Social Engineering tactic. Social Engineering is a term used to describe the practice of fraudsters manipulating a person or persons to obtain confidential information. This may include a telephone call or e-mail requesting the information directly, or requesting that the victim click on a malicious link. Here are some things to consider when it comes to avoiding the pitfalls of Social Engineering:

PHISHING

Phishing is a Social Engineering tactic in which fraudsters pose as trustworthy, and often authoritative, persons or organizations and request confidential information or that the victim visit a malicious website. These scams can be very elaborate and may include a completely fabricated website designed to mimic that of an actual organization. Never send confidential information via e-mail and investigate any messages you deem suspicious. Please keep in mind that phishing schemes often involve messages from the Better Business Bureau, IRS, FDIC, FBI, and other organizations.

E-MAIL SPOOFING & CORPORATE E-MAIL FRAUD

Just because an e-mail appears to be from a legitimate source, doesn't mean it is. Cybercriminals are capable of disguising the e-mail address a message is from. This means that although you may receive an e-mail from a *@midwestone.com* address or even a message from your own business' domain, it may not be coming from where it seems. **Fraudsters often send fake ACH or wire requests from spoofed e-mail addresses. They will pose as a member of your business's management or finance team, and may even include a bogus invoice, in an effort to trick an authorized user into submitting a payment request.**

The best thing to do is to practice due diligence; follow-up on suspicious requests by calling a telephone number you know to be legitimate. Do not use the telephone number from a suspicious e-mail. If you receive a suspicious message from someone at MidWest*One*, contact us at 1-800-247-4418.

SOCIAL ENGINEERING PREVENTITIVE TIPS

- Do not click on links in suspicious e-mails
- Be suspicious of unsolicited phone calls or e-mails
- Pay close attention to the sites you visit, malicious websites often mimic legitimate ones
- Do not share confidential information unless you are positive you know who it is you are talking to
- Take advantage of e-mail spam filters

Signs of a Corporate Account Takeover Attack

Here are some signs that a Corporate Account Takeover attack may be in progress against your business' online account:

- Untimely or unusual requests for login information, including a token one-time password
- Unusual pop-up messages, especially during online banking sessions
    - May include abrupt message about connection being lost
    - Often occurs after a password was successfully entered
- Changes in the way things appear on the computer screen
    - May be a new tool bar in the web browser
    - Fields being filled with characters without pressing any keys
- Computer freezing once online banking is accessed
- Inability to update security and/or OS programs
- Sudden computer slowness
- Unexpected rebooting of the computer

If you experience any of these problems, immediately exit the online banking session and contact us at 1-800-247-4418.

Frequently Asked Questions

What is MidWest*One* Bank doing to prevent fraud?

Balancing security and convenience can sometimes be a challenge; however, we believe we have implemented reasonable controls to protect your online account. These controls include the security tokens you use to access the service and a fraud monitoring system. If you don't have access to initiate ACH or wires online, you may not have a token.

Will MidWest*One* ever contact me to request my online banking login information?

No, we will not request your login information. However, we do use a fraud detection system for online banking. This means that, from time to time, we may contact you to verify recent activity.

What can I do to prevent fraud?

Review the security tips provided in this guide on page 4. Remain diligent, educate your employees, and use the appropriate security controls.

Who should I contact if I suspect fraud?

Contact us immediately at 1-800-247-4418 so that we can attempt to stop the fraudulent activity. Any sustained losses can be reported to law enforcement later.

What should I do if I suspect my computer is infected with malware?

Our recommendation is that you seek the assistance of an IT specialist. Also, contact us so that we may restrict online access to your account until the situation can be resolved.

What are the liabilities to my businesses? Will I get my money back?

A Corporate Account Takeover attack may be devastating to a business. Business account holders do not receive the same protection consumer account holders do under Regulation E, which is why it is so important for you to protect your electronic assets. Although it may depend upon the circumstances surrounding the cyber-attack, your business will likely be accountable for any lost funds. At MidWest*One* Bank, we take many precautions to prevent such attacks; however, we cannot be successful in preventing fraud unless you take the appropriate steps to protect your business as well.

The cybercriminals that carry out Corporate Account Takeover attacks have vast networks of mule accounts that enable them to rapidly disburse fraudulently collected funds. Should you become the victim of such an attack, we will do our best to recover the funds; however, large portions of funds send via unauthorized requests are often unrecoverable.

Additional Resources

NACHA CORPORATE ACCOUNT TAKEOVER RESOURCE CENTER

https://www.nacha.org/risk/sound-business-practices

The National Automated Clearinghouse Association's website dedicated to small business security.

STAY SAFE ONLINE

www.StaySafeOnline.org

See information specific for businesses computer security.

UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT)

www.US-Cert.gov

Find information regarding the latest threats and system vulnerabilities.

ONGUARD ONLINE

www.OnGuardOnline.gov

Get access to additional computer security information.

ANTI-PHISHING WORKING GROUP (APWG)

www.AntiPhishing.org

Find out about the latest trends in Social Engineering and phishing tactics.

MidWestOne has provided this link for your convenience, but is not responsible for the content, links, privacy policy, or security policy of this website. MidWestOne Bank is not endorsing, approving, certifying or controlling these sites and does not guarantee the accuracy, completeness, or timeliness of the information contained on the linked sites.

These links and more are available on our website at www.MidWestOne.bank/online-safety-tips