You're the *One*™

BUSINESS ONLINE BANKING SECURITY

Attention Business Online Cash Manager Users: The Threat of Corporate Account Takeover

Cybercriminals have been targeting the online accounts of small to medium sized businesses, non-profits, and municipalities. Corporate Account Takeovers are attacks carried out my cybercriminals that either obtain the login credentials or hijack the secure online session of a legitimate user through the use of malicious software. The criminals then initiate wire and 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. Therefore, it is essential that MidWest*One* Business Online Cash Manager users utilize proper computer security practices. Below are some tips regarding computer security for businesses.

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.

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 the computer is only used for online banking will drastically lower the chances of it becoming compromised via an infected e-mail or website.

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.

(Continued)

You're the One™

BUSINESS ONLINE BANKING SECURITY

(Continued)

Malware Protection / Anti-Virus Software
In addition to a Firewall, 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.

Update and Patch All OS, Business, & Security Programs Regularly
The security software protecting your business will be ineffective if it is not routinely updated. Any program your employees use, especially operating systems and web browsers, need to be updated and patched to protect against new threats.

Monitor Account Activity
If fraud does occur on your business accounts, it is important to catch it as soon as possible. At a minimum, check your accounts daily for unauthorized activity. Contact us immediately if you notice suspicious activity on a business account.

Additional Tips

- Enforce a strong workstation password policy
- Do not send confidential information through unencrypted e-mail
- Shut down or disconnect computers from the internet when not in use
- Educate your employees about avoiding phishing attacks and social engineering
- Backup your data