SECURITY

Keep your funds safe from Corporate Account Takeover and Security Risks.

Hometown Community Banks

Divisions of Morton Community Bank

Introduction

Keep your funds safe from Corporate Account Takeover and Security Risks.

Every day, millions of ACH transactions pass safely and securely through the banking system in the United States. The ACH process offers people and businesses a highly efficient, cost effective and simple method for moving funds quickly and securely.

As with almost any business process though, there are precautions which should be taken to help assure your activities remain safe.

Corporate Account Takeover

Corporate Account Takeover occurs when a criminal or criminal enterprise gains control of a business' bank account by stealing the business' valid online banking credentials. Although there are several methods being employed to steal credentials, the most prevalent involves phishing attempts to trick users into divulging their credentials to malicious websites. Once the credentials are stolen, a prevalent attack vector is one where malicious actors gain access to email accounts to research and then send sophisticated fraudulent email requests for money transfers.

What we do to minimize risk

The Bank provides each user with a customized set of security measures based on each user's activities and risk factors. Some of these measures include the use of a login token, Multi Factor Authentication based on the device used for access, minimum password complexity requirements, and/or automated telephone callback verification.

We also have a full-time staff who monitors ACH usage to help ensure that transactions are customary or expected for each customer.

What you should do to minimize risk

You should read and understand this security booklet. Discuss the various security risks and counter measures with your staff to be certain everyone has a clear understanding.

Complete the self-assessment form at the back of this booklet annually. If you need more copies, contact us and we will provide them.

Report any questionable activity to the Bank immediately.

Section 1

Overview

- How Thieves Obtain Your Data
- How Thieves Use Your Data

How Thieves Obtain Your Data

Criminals may attempt to compromise your credentials in a number of ways, such as:

- Tricking you into entering your Access ID and Password on a website that might look official... but really it is capturing the information you enter.
- Using viruses or Trojan programs to install spyware on your computer to capture your Access ID and Password and transmit them to the criminals.
- Pretending to be an official of a bank or other person whom you may trust.
- Pretending to be an employee of your own company.
- Searching through your paper trash.
- Physically accessing your computer.
- Stealing electronic devices, such as laptop computers, memory storage devices and cell phones.
- Using the position of an employee of your company.
- Convincing an employee of your company to join them.

Remember, identity thieves are not always strangers!

How Thieves Use Your Data

Thieves who take over your account electronically can do anything you can do...

They can see your accounts, look at your statements and check images, transfer funds among accounts and transfer funds out of your accounts if you have that ability.

If your business posts payments from customers or makes payments to vendors, you may even be placing those customers and vendors at risk if thieves obtain your log in credentials. If the thieves can see your transactions, they may be able to view information which can identify your customers or vendors. They can see how much you are paying or how much your company is getting paid.

Section 2

Types of Risks

- Executive Impersonation
- Ransomware
- Phishing
- Deepfake
- Fraudulent Emails
- Viruses and Trojans

Executive Impersonation

Business email compromise attacks use email fraud to attack commercial, government and non-profit organizations to achieve a specific outcome which negatively impacts the target organization. Typically, an attack targets specific employee roles within an organization by sending a spoof email (or series of spoof emails) which impersonate a senior level executive via an email, attempting to trick a member of an organization into sending money via ACH, wire or gift card purchase.

Ransomware

Ransomware is malicious software that is downloaded to a computer and then encrypts as much local and network data as fast as possible. The attackers usually send the malicious software via email, embedded in files like PDFs or office documents or via malicious clickable links within email messages. After files have been encrypted and rendered impossible to access, the malicious actors will usually demand a ransomware payment in the form of BitCoin in exchange for the decryption key.

Phishing

Phishing is an attempt to trick users into believing they are logging into a legitimate website. In the course of this attempted log in, the malicious actors can record the username and password entered and then use those stolen credentials to log in to secure locations with those stolen credentials. Phishing attempts are very common and typically arrive via email. Some attacks are incredibly sophisticated and difficult to distinguish as not being legitimate.

Deepfake

With the advent of high powered computers and Artificial Intelligence (AI) to generate deepfake audio and video, fraudsters are using software to impersonate the voice of a person authorized to initiate an ACH or wire transfer.

Fraudulent Emails

Fraudulent emails are a widely used ploy among identity thieves wanting to trick you.

Thieves may send you an email claiming you need to follow a link to reactivate your log in credentials or verify other information.

Commonly, these fraudulent emails claim your access has or will be deactivated unless you comply.

Our Bank will never send such an email. If you receive one, it is fraudulent.

Fraudulent emails may contain poor grammar or misspellings. However, some can be error-free and look very convincing.

Never click on a link in an email and then enter your credentials in the web page which opens. The web page may look like it belongs to your financial institution, but it does not. It is a forgery.

Even the URL in the address bar may look convincing, but it likely has a slight spelling change from the real URL address.

Viruses and Trojans

To gain control of your computer or intercept data, a thief may try to install malware.

Malware is a general term for programming that's harmful to your computer. It may be a virus or an actual program.

Malware can be used to capture information you type and send that information to a thief.

That malware may record your keystrokes, take pictures of your screen, or even allow someone else to watch remotely as you work.

The easiest way is for the thieves to send you a file which contains the malware or virus and get you to launch the file. They may send a file claiming to be a photo or a purchase order or some other document which you (naturally) would want to see. Any file, no matter how much you believe it to be safe, could contain harmful code and clicking on it could expose your system to a malicious actor.

Never plug an unknown USB flash stick into your computer because it also could contain malicious software. These files are called Trojans because they appear to be harmless yet have great harm hiding within them, just like the original Trojan Horse!

Malware can even be installed automatically if you visit an infected or malicious website.

Section 3

Other Security Risks

- Pretext Calling
- Dumpster Diving
- Physical Access to Your Computer
- Devices or Storage Media Theft

Pretext Calling

The person on the phone may not be who you think it is. Thieves may call you, pretending to be from your Bank or from some other department within your own company or even pretending to be an outside consultant.

Employees of larger companies sometimes can be fooled by receiving a phone call from someone claiming to be from the company's own computer department. The caller tries to get the employee to reveal network log in credentials or financial programs by pretending to be working on some sort of problem.

Thieves also may call pretending to be from your Bank. Again, they are trying to get the employee to reveal various credentials. Our Bank will never call and ask for confidential information.

The caller may even pretend to be your own customer or vendor.

No matter who the caller is claiming to be, you should not reveal any information at all!

Dumpster Diving

To identity thieves, your trash is a goldmine of information. It's just as easy to take something out of your trash bin as it is to place in the trash bin.

Thieves may be able to find user names and passwords in your discarded trash. They can find Bank statements, employee names...all sorts of information.

Even if they do not find confidential information, they may find documents which allow them to fool an employee with Pretext Calling. Something as innocent as a memo stating a computer upgrade will take place on a certain date may be all the thief needs. They simply wait until that date and then call an employee, pretending to be from the IT Department.

Even the seemingly innocent process of bagging your trash makes it easier for the thief. Instead of rooting through loose trash, the thief can simply grab a bag or two and take them someplace else to search through them!

Physical Access to Your Computer

Even a few moments with your computer can produce devastating results.

If a thief can physically access your computer, they can steal information by copying to a disk or flash drive, hand writing what they see on the screen, or even photographing the screen with a cell phone.

They can install malware intended to log your keystrokes or send information about your activities.

How would a thief gain access to your computer system? Perhaps by working with another person who distracts the receptionist or by waiting until an employee leaves for lunch. It could even be someone you would not suspect, such as an employee!

Devices or Storage Media Theft

As electronic devices grow smaller, the threat of theft grows larger. Stealing something small can be easier than stealing something large.

USB memory sticks are a little larger but possess all of the same risks.

CDs and DVDs are larger and just as thin and can be slipped among the pages of a book or in a jacket pocket.

Your **cell phone** can be a treasure trove of data and a thief who snatches your laptop computer has probably hit the mother lode.

Laptops are stolen from parked vehicles every day. If you are using a laptop in an airport and set it down and look away for a moment, it may well be gone when you turn back. In a case like that one, even having the laptop password protected may not help since the laptop was up and running when it was taken.

Section 4

Security Recommendations

- Toolbars
- Passwords
- Social Networks
- Anti Virus
- System and Program Updates
- Traffic Light Indicator

Toolbars

Try to avoid add-on toolbars as they offer little value. Many companies have created toolbars which can be added to common web browsers. You may not know exactly how they operate or what information they may be recording. Unless you are confident in your knowledge of computers, you may wish to avoid installing or using these toolbars.

Often, users will accidentally install a toolbar when downloading some sort of other program. As of July, 2016, people who downloaded the very useful Adobe Acrobat Reader program from Adobe's website had to uncheck a box manually to prevent the Google toolbar from downloading AND INSTALLING also.

Passwords

Your password is the key to your accounts. Keep it safe and private.

Passwords should never be written down. Do not let your computer or web browser remember passwords. Always use unique passwords for every site that requires credentials. Never tell anyone your password, even someone you trust... they may write it down or you may be overheard.

Be careful when you are changing your password. Is there anyone who could be watching? A cell phone could be used to record a video of someone changing a password. Later, the thief can take their time playing back the video and noting the keystrokes.

Passwords should be at least eight characters and should include:

- Upper case letters
- Lower case letters
- Numbers
- Special Characters

Passwords should not include any variation on your name, your initials, numbers associated with you, dictionary words or proper names. The best passwords are random, created via a random password generator.

Social Networks

Computers used for Cash Management should never be used to connect to social networking sites.
The most commonly known social networking sites are Facebook and Instagram but there are many others.

These networks may share more information about you than you want.

Additionally, certain applications available through these networks may not be safe. In many cases these applications, such as surveys and games, are not written by the social networking site. They are written by other users. These applications may contain malicious software or just be poorly written and cause problems with the operation of your computer.

Social Networks also can be a source for thieves to obtain personal information about a user. Armed with that information, they may try to impersonate an employee and attempt to get a password changed.

Anti Virus

Every computer, whether business or personal, should be equipped with a reliable anti virus program.

Anti virus programs should be updated at least once per day. Many users set their anti virus programs to check for updates as frequently as every hour. Generally, the automatic update feature requires the purchase of a subscription from the software company.

System and Program Updates

Best practice is to use supported software and keep it updated. Microsoft and Apple issue regular updates to their operating systems and software. Both companies offer an automatic update option and a scheduled update option.

With automatic updates, you set the system to connect on its own and download and install any needed updates. Usually the system will look for updates once per day.

Scheduled updates work the same and you can set a schedule you may prefer. The system will still connect automatically.

You also can run the update process manually, which is not recommended. Allowing automatic or scheduled updates assures the update process will not be forgotten.

Traffic Light Indicator

- Do not click on links in emails and then enter confidential information on the web pages that open.
- Do not give out confidential information to anyone who telephones you and claims to be from your bank.
- Do not use any computer for both Internet banking and file sharing or social networking.
- Do not have your computer “remember” your passwords.
- Do not send confidential information through ordinary Internet email.
- Do not install browser add-ons that are not needed.

- Use caution dealing with anyone on the phone, even someone claiming to be from your own company.
- Use caution when navigating to your bank log in page. Enter the address in the address bar or use a bookmark instead of using a search.
- Use caution when opening email attachments.
- Use caution with portable devices to protect them from theft.

- Do limit physical access to your computer.
- Do use a reliable anti virus program and keep it updated daily.
- Do keep your Access ID and Password secret.
- Do discard trash securely to protect sensitive information.
- Do keep your operating system and software updated.
- Do protect your portable computer with a complex start-up or log-in password.


VIRUS


User
••••••••

Section 5

Detection and Reporting

- Detecting a Corporate Account Takeover
- Taking Action on Suspicious Activity

Detecting a Corporate Account Takeover

You can protect yourself by being aware of the status of your computer and your very important accounts. Some warning signs that your computer may have been compromised include:

1. Inability to log into online banking. Thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money;
2. Dramatic loss of computer speed;
3. Changes in the way things appear on the screen;
4. Computer locking up so the user is unable to perform any functions;
5. Unexpected rebooting or restarting of the computer;
6. Unexpected request for a one time password (or token) in the middle of an online session;
7. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.);
8. New or unexpected toolbars and/or icons;
9. Problems with your anti virus program, such as the icon indicating it is turned off; and
10. Inability to shut down or restart the computer.

Try to keep a watchful eye on your account activity. Activity you did not expect or do not understand may indicate unauthorized use of your account. Review your accounts online at least once a day, paying particular attention to internal transfers and debits to the account.

In some cases, no one employee may know about all the expected account activity details. Accounts Payable and Payroll may be functions performed by different departments and each of those departments may not be aware of the activity generated by the other.

You may wish to assign a **single** department the responsibility of daily review of the account activity and have other departments report to them the activity they generated.

Taking Action on Suspicious Activity

The key to a swift response is taking appropriate and timely action. If you find unexplained activity in your account:

1. Call the bank immediately.
2. Report the date of the transaction, the type and the amount.
3. If you suspect the unauthorized activity may have occurred through the Internet, inform your IT Department or your technology consulting firm.

The Bank may be able to stop the transaction. Be certain that you have the authority to request the bank do so.

The Bank will not report the activity to the police. Reporting the activity to the police is your responsibility. The Bank recommends you file a police report. The local police may ask that you contact another agency, such as the FBI. It is not unusual for the FBI to become involved in such matters.

If you suspect your computer may have been compromised - even if there has been no suspicious account activity:

1. Call the Bank and ask that your password be changed or that access to your accounts via computer be locked.
2. Stop using the suspect computer and turn it off.
3. Inform your IT Department or your technology consulting firm.

Your IT Department or technology consulting firm will likely examine the suspect computer to determine if it has been compromised. If it has been compromised with malware, the decision to reprogram or replace the computer is yours. Remember, some malware programs can be very difficult to detect and very difficult to remove. Sometimes, it can appear malware has been removed, but it remains in hiding and reactivates at a later date.

Report to the Bank if malware has been found. There are steps the Bank can take to assist in protecting your account.

If you determine a computer has been compromised and if you can determine how it happened, you may wish to review your own internal controls and policies to try to prevent a future re-occurrence.

Section 6

Your Security Checklist

- General Security
- Computer Operating System
- Internet
- Intrusion Protection

This self-evaluation form will aid in determining if your systems and practices are providing the proper protection against Corporate Account Takeover.

Preferred or recommended answers are in bold. The remaining questions are intended to assure that you are sufficiently acquainted with your system to be able to guard against fraud.

This form, or one similar, should be completed annually or after any major changes in your computer or office systems.

General Security

Is the computer kept in an area inaccessible by the public?
o Yes o No

Does the computer automatically lock when inactive?
o Yes o No

Do users share Access ID's for internet banking?
o Yes o No

Do users keep written copies of their log in credentials?
o Yes o No

Are employees allowed to access the system remotely?
o Yes o No

Is the screen oriented in a way that other persons can see it?
o Yes o No

Do users log off at the end of the workday?
o Yes o No

Are passwords required to be complex?
o Yes o No

Do any persons other than employees use the computer?
o Yes o No

Have you enabled MFA - Multi-Factor Authentication?
o Yes o No

Are you using a unique password for Online Banking?
o Yes o No

Computer Operating System

What is the operating system?

o Windows 7 o Windows 8.1
o Windows 10 o Windows Newer
o OS X 10.10 o OS X 10.11
o OS X 10.12 o Apple Newer
o Linux o Other_____

How is the operating system updated?

o Automatic Daily o Automatic Weekly
o Automatic Monthly o Manually o Never

Internet

Internet Browser:

o Firefox o Microsoft Edge
o Safari o Chrome Version:_____
These browsers are the only ones supported.

Are any add-on tool bars such as Yahoo or Google installed?

o Yes o No

Is the computer used to connect to social networking sites?

o Yes o No

Is the computer used for any online game playing?

o Yes o No

Is any web filtering appliance or program in use?

o Yes o No

Is your email service an online provider, such as Yahoo or Gmail?

o Yes o No

Is personal use of the internet permitted?

o Yes o No

Does the browser remember log in credentials?

o Yes o No

Intrusion Protection

Is there a Firewall?

o Yes o No

Name: _____Version:_____

Is there an Anti-Virus program?

o Yes o No

Name: _____Version:_____

How often does the Anti-Virus program update virus definitions?

o Every Day o Every week

o Every Month o Never

How often does the Anti-Virus program automatically scan the system?

o Every Day o Every week

o Every Month o Never

Does the Anti-Virus program scan emails?

o Yes o No

Is there an Anti-Spyware program?

o Yes o No

Name: _____Version:_____

Does the Anti-Spyware program scan all downloads?

o Yes o No

Completed By: _____

Date: _____

Notes

Hometown
Community Banks
Divisions of Morton Community Bank
Member FDIC

Version 1.0 | 09-2021