Resource Documents for Additional Information

Fraud Advisory for **Businesses**: Corporate Account Take Over

This product was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Problem:
Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered[1].

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

Figure 1: Recent news headlines from *The New York Times*, *The Washington Post*, *Computer World*, and *Krebs on Security*.

To obtain access to financial accounts, cyber criminals target employees– often senior executives or accounting and HR personnel[2]- and business partners[3] and cause the targeted individual to spread

[1] Consumer accounts are subject to Federal Reserve Regulations E (12C.F.R. Part 205) which requires banks to provide reimbursement for certain losses. Regulation E does not apply to business accounts. Therefore, banks are not required to provide reimbursement for certain losses.
[2] *Any* employee is vulnerable to being targeted.

malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts. Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information - often through the spread of malware - that can also cause indirect losses and reputational damage to a business.

First identified in 2006, this fraud, known as "corporate account take over," has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses, and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Educating all stakeholders (financial institutions, businesses and consumers) on how to identify and protect themselves against this activity is the first step to combating cyber criminal activity.

This advisory was created by financial institutions, industry trade associations, Federal law enforcement and regulatory agencies.[4] It is intended to make businesses aware of this issue, identify some examples of how the fraud may occur, and provide updated recommendations to businesses to protect themselves against it. The information contained in this advisory is intended to provide basic guidance and resources for businesses to learn about the evolving threats and to establish security processes specific to their needs. However, it is very important to note that as the cyber criminals change their techniques, businesses must continue to improve their knowledge of and security posture against these attacks. In addition, the tips and recommendations contained in this advisory may help reduce the likelihood of fraud, but they should not be expected to provide complete protection against these attacks.

How it's Done:

Cyber criminals employ various technological and non-technological methods to manipulate or trick victims into divulging personal or account information. Such techniques may include performing an action such as opening an email attachment, accepting a fake friend request on a social networking site, or visiting a legitimate, yet compromised, website that installs malware on their computer(s).

[3] Business partners can include, among other third parties, contractors and accountants.

[4] This advisory was created through a collaborative cross-industry effort to develop and distribute recommended practices to prevent, detect and respond to corporate and consumer account takeovers. Led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), contributors include more than 30 of the largest financial institutions in the U.S., industry associations including the American Bankers Association (ABA), NACHA - The Electronic Payments Association, BITS/The Financial Services Roundtable; and federal regulatory and law enforcement agencies.

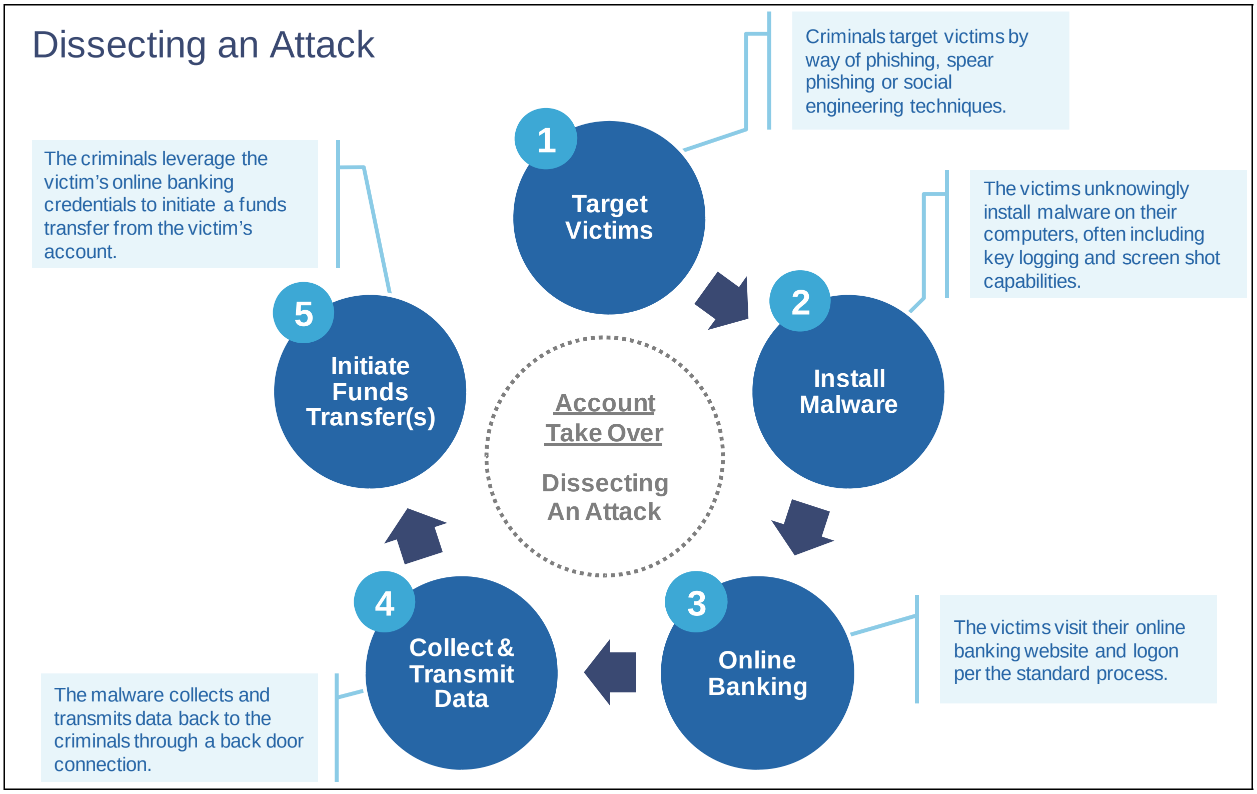
Dissecting an Attack
Criminals target victims by way of phishing, spear phishing or social engineering techniques.
1
Target Victims
The victims unknowingly install malware on their computers, often including key logging and screen shot capabilities.
2
Install Malware
3
Online Banking
The victims visit their online banking website and logon per the standard process.
4
Collect & Transmit Data
The malware collects and transmits data back to the criminals through a back door connection.
5
Initiate Funds Transfer(s)
The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.
Account Take Over
Dissecting An Attack

Figure 2: **Dissecting An Account Take Over Attack**

Cyber criminals will often "phish" for victims using mass emails, pop-up messages that appear on their computers, and/or the use of social networking and internet career sites[5]. For example, cyber criminals often send employees unsolicited emails that:

- Ask for personal or account information;
- Direct the employee to click on a malicious link provided in the email; and/or
- Contain attachments that are infected with malware.

Cyber criminals use various methods to trick employees into opening the attachment or clicking on the link, including:

- Disguising the email to look as though it's from a legitimate business. Often, these criminals will employ some type of scare tactic to entice the employee to open the email and/or provide account information. For example, cyber criminals have sent emails claiming to be from:
  1. UPS (e.g., "There has been a problem with your shipment.")
  2. Financial institutions (e.g., "There is a problem with your banking account.")
  3. Better Business Bureaus (e.g., "A complaint has been filed against you.")
  4. Court systems (e.g., "You have been served a subpoena.")

- Making the email appear to provide information regarding current events such as natural disasters, major sporting events, and celebrity news to entice people to open emails and click on links.

[5] Cyber criminals also use "vishing", which is soliciting victims over the phone or Voice over IP (VoIP).

- Using email addresses or other credentials stolen from company websites or victims, such as relatives, co-workers, friends, or executives and designing an email to look like it is from a trusted source to entice people to open emails and click on links.

The cyber criminal's goal is to get the employee to open the infected attachments or click on the link contained in the email and visit the nefarious website where hidden malware is often downloaded to the employee's computer. This malware allows the fraudster to "see" and track employee's activities across the business' internal network and on the Internet. This tracking may include visits to your financial institution and use of your online banking credentials used to access accounts (account information, log in, and passwords). Using this information, the fraudster can conduct unauthorized transactions that appear to be a legitimate transaction conducted by the company or employee.

How to Protect, Detect, and Respond

Protect

1. **Educate everyone on this type of fraud scheme**
    - Don't respond to or open attachments or click on links in unsolicited e-mails. If a message appears to be from your financial institution and requests account information, do not use any of the links provided. Contact the financial institution using the information provided upon account opening to determine if any action is needed. Financial institutions do not send customers e-mails asking for passwords, credit card numbers, or other sensitive information. Similarly, if you receive an email from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.) contact the sender directly through other means to verify the authenticity. Be very wary of unsolicited or undesired email messages (also known as "spam") and the links contained in them.
    - Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.
    - Teach and require best practices for IT security. See #2, "Enhance the security of your computer and networks".

2. **Enhance the security of your computer and networks to protect against this fraud[6]**
    - Minimize the number of, and restrict the functions for, computer workstations and laptops that are used for online banking and payments. A workstation used for online banking should not be used for general web browsing, e-mailing, and social networking. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.
    - Do not leave computers with administrative privileges and/or computers with monetary functions unattended. Log/turn off and lock up computers when not in use.
    - Use/install and maintain spam filters.

[6] See the "Resources" section for links to helpful and detailed tips on how to enhance your information technology (IT) security.

- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software.
  - Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network.
  - Change the default passwords on all network devices.
- Install security updates to operating systems and all applications, as they become available. These updates may appear as weekly, monthly, or even daily for zero-day attacks.
- Block pop-ups.
- As recommended by Microsoft for users more concerned about security, many variants of malware can be defeated by using simple configuration settings like enabling Microsoft Windows XP[7], Vista[8], and 7 Data Execution Prevention (DEP)[9] and disabling auto run commands[10]. You may also consider disabling JavaScript in Adobe Reader[11]. If these settings do not interfere with your normal business functions, it is recommended that these and other product settings be considered to protect against current and new malware for which security patches may not be available.
- Keep operating systems, browsers, and all other software and hardware up-to-date.
- Make regular backup copies of system files and work files.
- Encrypt sensitive folders with the operating system's native encryption capabilities. Preferably, use a whole disk encryption solution.
- Do not use public Internet access points (e.g., Internet cafes, public wi-fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN)[12].
- Keep abreast of the continuous cyber threats that occur. See the Additional Resources section for recommendations on sites to bookmark.

3. Enhance the security of your corporate banking processes and protocols

- Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system. This helps ensure that one person does not have the access authority to perform both functions, add additional authority, or create a new user ID.

[7] How to configure memory protection in Windows XP SP2; http://technet.microsoft.com/en-us/library/cc700810.aspx

[8] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows-vista/Change-Data-Execution-Prevention-settings

[9] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows7/Change-Data-Execution-Prevention-settings

[10] How to disable the Autorun functionality in Windows: http://support.microsoft.com/kb/967715/

[11] Disabling JavaScript in Adobe Reader and Acrobat; http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html

[12] A VPN uses the public telecommunication infrastructure and the Internet to provide remote and secure access to an organization's network.

- Talk to your financial institution about Positive Pay and other services such as SMS texting, call backs, and batch limits which help to protect companies against altered checks, counterfeit check fraud and unauthorized ACH transactions.
- If, when logging into your account, you encounter a message that the system is unavailable, contact your financial institution immediately.

4. **Understand your responsibilities and liabilities**
   - Familiarize yourself with your institution's account agreement**.** Also be aware of your liability for fraud under the agreement and the Uniform Commercial Code (UCC), as adopted in the jurisdiction, as well as for your responsibilities set forth by the Payment Card Industry Data Security Standard (PCI DSS), should you accept credit cards. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Detect

5. **Monitor and reconcile accounts at least once a day**
   - Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity and allows the business and the financial institution to take action to prevent or minimize losses.

6. **Discuss the options offered by your financial institution to help detect or prevent out-of-pattern activity (including both routine and red flag reporting for transaction activity).**

7. **Note any changes in the performance of your computer such as:**
   - A dramatic loss of speed.
   - Changes in the way things appear.
   - Computer locks up so the user is unable to perform any functions.
   - Unexpected rebooting or restarting of your computer.
   - An unexpected request for a one time password (or token) in the middle of an online session.
   - Unusual pop-up messages.
   - New or unexpected toolbars and/or icons.
   - Inability to shut down or restart.

8. **Pay attention to warnings**
   - Your anti-virus software should alert you to potential viruses. If you receive a warning message, contact your IT professional immediately.

9. **Be on the alert for rogue emails**
   - If someone says they received an email from you that you did not send, you probably have malware on your computer.
   - You can also check your email "outbox" to look for email that you did not send.

10. **Run regular virus and malware scans of your computer's hard drive**
    - This can usually be set to run automatically during non-peak hours.

Respond

11. **If you detect suspicious activity, immediately cease all online activity and remove any computer systems that may be compromised from the network.**
    - Disconnect the Ethernet cable and/or any other network connections (including wireless connections) to isolate the system from the network and prevent any unauthorized access.

12. **Make sure your employees know how and to whom to report suspicious activity to within your company and at your financial institution**

13. **Immediately contact your financial institution so that the following actions may be taken:**
    - Disable online access to accounts.
    - Change online banking passwords.
    - Open new account(s) as appropriate.
    - Request that the financial institution's agent review all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, cancel them immediately.
    - Ensure that no one has added any new payees, requested an address or phone number change, created any new user accounts, changed access to any existing user accounts, changed existing wire/ACH template profiles, changed PIN numbers or ordered new cards, checks or other account documents be sent to another address.

14. **Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, financial institutions, and firms impacted**
    - Be sure to record the date, time, contact telephone number, person spoken to, instructions, and any relevant report or reference number.

15. **File a police report and provide the facts and circumstances surrounding the loss**
    - Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often help facilitate the filing of claims with insurance companies, financial institutions, and other establishments that may be the recipient of fraudulent activity.
    - The police report may result in a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender, and possibly recovering losses.
    - Depending on the incident and the circumstance surrounding the loss, investigating officials may request specific data be recorded and some or all of the system's data may need to be preserved as potential evidence.
    - In addition, you may choose to file a complaint online at www.ic3.gov. For substantial losses, contact your local FBI field office (http://www.fbi.gov/contact-us/field/field-offices), your local United States Secret Service field office

(http://www.secretservice.gov/field_offices.shtml), or the Secret Service's local Electronic Crimes Task Force (http://www.secretservice.gov/ectf.shtml).

16. Have a contingency plan to recover systems suspected of compromise

- The contingency plan should cover resolutions for a system infected by malware, data corruption, and catastrophic system/hardware failure. A recommended malware removal option is to reformat the hard drive, then reinstall the operating system and other software on the infected computer(s). There is no preservation of data using this method – all your data will be permanently erased. Do not take this step until you determine if a forensic analysis of the computer is needed. For additional recommendations on steps to take following a compromise, see the section "What if I am Compromised" on page 6 of the US CERT document, *Malware Threats and Mitigation Strategies* available at http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf

17. Consider whether other company or personal data may have been compromised

18. Report exposures to PCI DSS.

- If your business accepts credit cards, you are subject to compliance with the Payment Card Industry Data Security Standard (PCI DSS) and you may be required to report and investigate the incident, limit the exposure of the cardholder data, and report the incident to your card company. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Contact your financial institution for more information.

Additional Resources:

- Federal Trade Commission (FTC) website, "Computers& the Internet: Privacy and Security"[13] (includes OnGuard Online),
- Internet Crime Complaint Center (IC3)[14],
- Department of Homeland Security Cyber Report[15],
- National Cyber Security Alliance Stay Safe Online[16].
- Better Business Bureau- "Data Security Made Simple"[17]
- Microsoft Security Page[18]
- U.S. Chamber of Commerce's "Internet Security Essentials for Small Business"[19]

[13] http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm

[14] The IC3 is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). For more information, see http://www.ic3.gov/default.aspx.

[15] http://www.cyber.st.dhs.gov/

[16] http://www.staysafeonline.org/

[17] http://www.bbb.org/data-security/

[18] http://www.microsoft.com/security/default.aspx

[19] This document is scheduled for release on October 26, 2010. Visit www.uschamber.com/cybersecurity for more information.

Sound Business Practices for Companies to Mitigate Corporate Account Takeover

I. Executive Summary

Corporate Account Takeover is a type of business identity theft in which a criminal entity steals a company's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business can fall victim to these crimes.

Attacks today are typically perpetrated quietly, by the introduction of malware through a simple email or infected website. For businesses that have low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks and even months. Introducing layered security processes and procedures, technological and otherwise, and other tightened security efforts, can help protect businesses from criminals seeking to drain accounts and steal confidential information. These increased security procedures may help reduce the incidence of, and mitigate the financial losses, business risks, and reputational damage that can result from such attacks.

NACHA's Risk Management Advisory Group has developed the following sound business practices for companies of all sizes to consider when reviewing and implementing security procedures to mitigate the threat of Corporate Account Takeover. The sound business practices outlined in this paper are not meant to be taken as the exclusive approaches businesses should implement to address the risks associated with Corporate Account Takeover, nor are they meant to be considered mandatory requirements. No single security measure alone is likely to be effective in preventing or mitigating all risks associated with Corporate Account Takeover. Similarly, some of these sound business practices may not be appropriate for all businesses. Accordingly, each business must identify its own risks, and design and implement the appropriate security measures to prevent, and mitigate the risks associated with Corporate Account Takeover.

The sound business practices for companies outlined in this document are:

Computer Security:

- Layered System Security
- Online Banking Safety
- Education
- Websites
- User Accounts
- Staying Informed

Account Security:

- Dual Control
- Reconcilement
- Account Services
- Reporting of Suspicious Activity
- Credentials

II. Sound Business Practices

Each business should evaluate its risk profile with regard to Corporate Account Takeover and develop and implement a security plan, including sound business practices, to prevent and mitigate the risk of Corporate Account Takeover. Such plan should be appropriate to the unique circumstances of the business. However, in developing such a plan, each business should consider the following sound business practices, which are recommended in most cases, and any other sound business practices determined by the company regardless of whether such practices have been communicated by NACHA.

Computer Security

Layered System Security

It is recommended that a business:

- Use appropriate tools to prevent and deter unauthorized access to its network and periodically review such tools to ensure they are up-to-date. These tools include:
    - Firewalls
    - Security suites
    - Anti-botnet, anti-malware, and anti-spyware programs
    - Encryption of laptops, hard drives, VPN's or other communications channels
    - Education of all computer users

- Install robust anti-virus and security software for all computer workstations and laptops and ensure that such software automatically is patched regularly and remains current.

- Implement multi-layered system security technology. Anti-virus software, alone, will not protect a business from most threats. Layering security software constructs a multi-level barrier between business' networks and criminals attempting to access such networks.

- Implement security suites so all security options (i.e., firewall, anti-virus, anti-spyware, anti-malware, etc.) work harmoniously to provide superior protection since security programs from multiple companies sometimes do not work well together, often working against each other which could leave the computers just as vulnerable as if they had no protection.

Online Banking Safety

It is recommended that a business:

- Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.

- Disallow a workstation used for online banking to be used for general Web browsing and social networking.

- Verify use of a secure session ("https") in the browser for all online banking.

- Disallow the conduct of online banking activities from free Wi-Fi hot spots like airports or Internet cafes.

- Cease all online banking activity if the online banking application 'looks' different than usual. Do not continue and contact the financial institution immediately.

Education

It is recommended that a business:

- Educate all computer users about cybercrimes so everyone understands that even one infected computer can lead to an account takeover.

  A user whose computer becomes infected can infect the entire network. For example, if an employee takes their laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business' entire network when the employee connects at work. All users, even those with no financial responsibilities, should be educated about these threats.

- Always ask, "Does this email or phone call make sense?"

  - Educate all of its employees to think critically about each email and phone call received. A business should advise its employees to:

    - Not open suspicious emails or emails from unknown persons. Even opening an email may expose a computer and the network to malware.

    - Ask, "Does this make sense?" before taking action in response to an email. If an email is suspicious, do not click on the link or open the attachment. The link can take the user to an infected website or download a malware program. Likewise, attachments and .zip files (compressed files) can contain malware. Users should be instructed to simply delete the suspicious email and not to click the link or open the attachment. The business also can inquire of a domain lookup service like "whois.net" or similar service that allows users to view the domain registration information of an email sender. If the user does not stop to think and take appropriate action, criminals may be able to lure an unsuspecting user into an action that may infect their computer.

    - Be particularly suspicious of emails or calls purporting to be from a financial institution, government agency or other organization requesting account information, account verification or banking access credentials such as usernames, passwords, Personal Identification Numbers (PINs) and similar information. If such a suspicious email is identified or call received, the business should call the financial institution to verify legitimacy. The business should not call the phone number included in the email, click on the link or reply to the sender of such an email.

Websites

It is recommended that a business:

- Block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit during work hours. Common sites that carry a high-risk are adult entertainment, online gaming, social networking, and personal email.

User Accounts

It is recommended that a business:

- Establish user accounts for every computer and limit administrative rights. Many malware programs require the user to have network administration privileges to infect the computer.

- Employ "user" settings to avoid accidentally downloading a credential-stealing program. Many small and mid-sized businesses allow all employees to be the network administrator of their computer. Most malware requires the user to be logged in as the network administrator for the malicious program to download.

- Require all employees use strong passwords and change their passwords frequently on both the computer and online banking access.

- Promptly deactivate or remove access rights from employees that no longer require access (e.g., inactive, transferred or terminated employees).

- Take full advantage of options offered by financial institutions to reduce the risk of a large payment being initiated fraudulently. Many financial institutions allow customers to set a "user limit" for ACH and wire transfer initiation via their online banking portal.

Staying Informed

It is recommended that a business:

- Stay informed about defenses to Corporate Account Takeover. Since cyber threats change rapidly, it is imperative that all businesses stay informed about evolving threats and adjust security measures timely. Among other things, this can be done by connecting with alert groups, businesses and industry resources about threats and frauds.

Account Security

Dual Control

It is recommended that a business:

- Initiate payments under dual control, with assigned responsibility for transaction origination and authorization. Dual control involves file creation by one employee with file approval and release by another employee on a different computer. Or, require dual use of tokens where a single employee creates a file, but can only release the same file by logging in a second time using a new passcode on the token. Avoid having employees initiate and authorize payment transactions with administrator credentials.

Reconcilement

It is recommended that a business:

- Reconcile accounts online daily; at a minimum, review pending or recently sent ACH files and wire transfers.

Account Services

It is recommended that a business:

- Take advantage of appropriate account services offered by its financial institution. Financial institutions offer a variety of services like positive pay, security tokens, debit blocks, call-backs, etc. Consult your financial institution to identify what security services it offers.

- Use multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. Multi-factor authentication includes at least two of the following: 1) something the person knows (user ID, PIN, password), 2) something the person has (password-generating token, USB token), and 3) something the person owns (biometrics, i.e., fingerprint scan).

Reporting of Suspicious Activity

It is recommended that a business:

- Monitor and report suspicious activity. Ongoing monitoring and timely reporting of suspicious activity are crucial to deterring or recovering from these frauds. A business should report anything unusual to the financial institution, such as log-ins at strange times of day, new user accounts, unauthorized transfers, etc., so the financial institution can immediately block the account and monitor activity.

Credentials

It is recommended that a business:

- Not use administrator credentials issued by its financial institution for day-to-day processing. Criminals use compromised administrator rights to create new users to perpetrate frauds. If criminals gain access to these credentials, they will set up their own users and profiles on your system to facilitate fraudulent transactions. The criminals can even use the administrator credential to lock legitimate users out of the system.

FDIC Consumer News Frauds Target Small Businesses

FDIC Consumer News

Frauds Target Small Businesses: Don't Be a Victim

While large firms may have sophisticated technology and staff dedicated to thwarting crime, many small businesses don’t — and scammers know this. Here are ways to protect yourself:

Be on guard against inside jobs. This includes employee theft or misuse of cash, merchandise or equipment as well as fraud. “Minimize risks through steps such as pre-employment background checks, automated inventory tracking systems, audits, and clearly outlined policies for personal use of computers and other business equipment,” said Luke W. Reynolds, Chief of the FDIC’s Outreach and Program Development Section. “Also, carefully select who handles revenue from customers, pays the bills and reviews account statements. And, ensure that there are procedures in place to detect and deter fraud.”

Watch out for fraudulent transactions and bills. Scams can range from consumer payments with a worthless check or a fake credit or debit card to fraudulent returns of merchandise. Be sure you have insurance to protect against risks. Also ignore offers to buy lists of federal grant programs. To learn more about protecting your business, consult your local Small Business Administration District Office (www.sba.gov/content/find-local-sba-office).

Electronic frauds by third parties can be very costly to businesses, so take them seriously. The FDIC has seen an increase in reports of unauthorized electronic transfers made from bank accounts held by small businesses. “The most common and dangerous scam for small businesses is account takeover,” said Michael Benardo, Chief of the FDIC’s Cyber-Fraud and Financial Crimes Section. “By sending fake e-mails and using fake Web sites to deliver malicious software, such as keystroke loggers, fraudsters may be able to obtain the IDs and passwords for online bank accounts and then make withdrawals from accounts.”

Because businesses are generally not covered by federal consumer protections against unauthorized electronic fund transfers, a bank likely will not be responsible for reimbursing losses associated with the theft from the account if it says that negligence on the part of the business, such as falling for a common scam, was a factor.

Also equip your computers with up-to-date anti-virus software and firewalls (to block unwanted access). Make backup copies of critical business data on every computer. Also monitor account balances regularly, perhaps daily, to look for suspicious or unauthorized activity.

And, don’t click on links in or attachments to an unsolicited e-mail that asks for confidential information, even if it appears to be from a company you do business with or the government. Legitimate organizations won’t request that kind of information in an e-mail. When in doubt, go to another source to find the organization’s contact information so you can independently confirm the validity of the request.

To check out a variety of frauds targeting small businesses and what you can do to stop them, visit the scam alert page at www.usa.gov/topics/consumer/scams-fraud/business/small-business-scams.shtml.

Scam Alert: Targeting Small Business

- BBB Warns Small Business Owners to Beware of Telephone Relay Fraud
  Better Business Bureau warns small business owners that reports of scammers plying their trade through telephone relay services -- typically used by the hearing impaired to make phone calls -- are cropping up all across the country. BBB has received reports from many types of businesses that received suspicious orders through TTY or telephone relay services.
- Beware of Phony Invoices
  Unauthorized invoices and unordered merchandise continue to show up at places of business across British Columbia due to some misleading telemarketing tactics. Better Business Bureau would like to advise businesses that they need a trained and prepared staff for handling these slick sellers.
- Businesses Beware of Mass Marketing Scams
  Illicit mass marketers know that the keepers of corporate funds may be just as susceptible to fake ploys as anyone else. And while business-oriented fraud usually results in losses of a few hundreds dollars the first time a company is hit, employees may continue to fall victim to these scams if the company has insufficient internal controls. Read on to learn more about the mass marketing frauds that are perpetrated against businesses and the steps a business can take to protect themselves.
- Fraudulent E- Mails Claiming to Be From the FDIC
  The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being from the FDIC.
- Seven Scams that Target Small Businesses
  Being vigilant against fraud is not only important for a company's bottom line, it also strengthens customer trust in the business. Becoming a victim of fraud can have a negative financial and reputational impact on a business and the Better Business Bureau recommends owners train their staff to look out for seven common scams that prey on small companies.

Ten Cybersecurity Tips for Small Businesses

FCC

STOP | THINK CONNECT™

Broadband and information technology are powerful tools for small businesses to reach new markets and increase sales and productivity. However, cybersecurity threats are real and businesses must implement the best tools and tactics to protect themselves, their customers, and their data. Visit ***www.fcc.gov/cyberplanner*** to create a free customized Cyber Security Planning guide for your small business and visit ***www.dhs.gov/stopthinkconnect*** to download resources on cyber security awareness for your business. Here are ten key cybersecurity tips to protect your small business:

1. Train employees in security principles. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. Protect information, computers, and networks from cyber attacks. Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. Provide firewall security for your Internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. Create a mobile device action plan. Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. Make backup copies of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6. Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

9. Limit employee access to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Passwords and authentication. Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

The FCC's Cybersecurity Hub at http://www.fcc.gov/cyberforsmallbiz has more information, including links to free and low-cost security tools. Create your free small business cyber security planning guide at www.fcc.gov/cyberplanner.

To learn more about the Stop.Think.Connect. Campaign, visit www.dhs.gov/stopthinkconnect.