Quincy Credit Union
Corporate Takeover Account Plan

Corporate Account Takeover Guide (CATO)

This guide was created to increase our Member's awareness of the potential risks and threats that are associated with Internet and electronic-based services and to provide solutions and tools to help prevent fraud and scams.

Corporate **A**ccount **T**ake**o**ver is a growing form of electronic crime where thieves typically use some form of malware, or malicious software, to obtain login credentials to corporate online banking accounts and fraudulently transfer funds from the accounts. Another means fraudsters commonly employ is phishing, masquerading as a trustworthy entity in an electronic communication or through social engineering to gain access to your sensitive information.

These attacks can result in substantial monetary loss for your company that, often, cannot be recovered. As a financial institution, we do everything we can to keep your money safe. Unfortunately, our security practices can only go so far to protect your accounts from corporate account takeover. There are some vulnerabilities that can only be addressed from your side and therefore require that the business implement sound practices with their Staff, systems and offices.

The following sections are contained in this Guide:

- General information on how CATO fraud work
- Sound Business Practices to combat this threat
- Education & Internet Risk Awareness
- Security
    - Computer
    - Account
    - User
- Detection and Response
- Explanation of Potential Liability
- Other resources

1. HOW DOES CATO FRAUD HAPPEN?

CATO attacks do not target the security systems or computers of the financial institutions; instead these attacks seek to find Members that have the ability to initiate funds transfers from their accounts using their computers. The goal is to obtain the Member's access codes, (user name and password), without the Member's knowledge so they will continue to be active and the fraudster can perform financial transactions impersonating the Member. A common way this is done is to get the Member to click on a link in an email, website or pop-up that installs a malware program on the Member's computer. The malware will secretly record the Member's activity and use a "key-logger" to record the user names and passwords as they are entered when logging into a banking site. This information is either retrieved by the fraudster using a remote connection opened by the malware or sent to their computer for them to use remotely. They may also compromise the email accounts of the user to send transfer requests from the Member's email account. Other computer information is also stolen such as security cookies or other information to allow the fraudster to logon to the Credit Union's system to make everything appear to look like they are the actual user.

In some cases, the fraudster may use "social engineering" as the way to get this information. To do this, the fraudster may place a call or send an email and claim to be from the Credit Union or another trusted source and requests the information as part of a trouble-shooting effort. Many times it is done with an email that claims the user must update their account information or confirm a password due to a problem or security alert that appears to be from a financial institution.

Once the fraudster has the Member's banking credentials (login and password), they will logon to the banking sites. QCU does not allow Wire Transfers or ACH transfers online. Transactions that may occur during this time is to move money through Account-to-Account; ($2,500) People-to-People; ($2,500) Bill Payment services or Remote Deposit Capture. These methods are the primary ones selected because they can send large amounts of money and the funds are immediately available for withdrawal when received or on the next day. The money may go straight to the fraudster, but more often it will go to a person that has been recruited to receive and immediately forward the funds to the crooks. The "money-mule" will typically not know they are part of a fraud and responded to an employment or other advertisement on the web that promised they can keep a handling fee. This trick keeps the fraudster's identity and location out of the transaction. Once the money has been withdrawn, recovery is nearly impossible due to the banking rules.

After the discovery of the fraudulent transactions, the business and the Credit Union will need to work together to try to recover funds. In most cases, there will be an amount that cannot be recovered and represent a loss to either the Member or financial institution. There are currently no clear rules on who will suffer the loss in these situations. Many losses have been settled on a case-by-case basis depending on the entity that had its security responsibility breached by the compromise. In cases where a business fails to use any of the recommended security procedures offered by the Credit Union or has lax internal security and controls, they have often been held to absorb all or a portion of the liability for the loss.

2. SOUND BUSINESS PRACTICES THAT CAN HELP PREVENT CATO LOSSES

We have outlined some ideas on areas or tools that can be used to thwart fraudsters that want to attack your business or staff. Although even if every suggestion or recommendation is adopted by the business; a potential for a Member's account to be compromised will be present. The Credit Union is constantly working to add other security measures on our side to proactively detect suspicious activity or perform other security reviews and out-of-wallet confirmations prior to allowing the completion of a funds transfer. Here are some security measures we urge you to take to safeguard your business from fraud.

2 a. **EDUCATION & INTERNET RISK AWARENESS**

The battle begins with creating a work environment where the Staff is aware of the threats posed by using the internet and how it is a doorway into the computer network of the company. Sharing this document can help educate your employees about cybercrimes and other means fraudsters may attempt to steal access to the business' accounts.

It is everyone's job to help keep the computer systems secure from Fraudsters. Even a laptop or home computer that has remote access to the network can allow hackers access if the user's PC is compromised and has sufficient network rights. Below are some tips that should be shared with the staff:

- **Think!** Responding to any call or email, first ask yourself, "Does this email or phone call make sense?"
- **Deny!** Never provide your user ID and password to anybody.
- **Distrust!** Do not trust ANY email, internet site, link or caller unless you know for sure it is legitimate
- **Conduct Training Sessions and Stay Current:** Hold staff training about the risks and keep up with news articles or fraud awareness updates.
- **Link Avoidance**. Never click on a link in an email or internet site unless you know for sure it is legitimate
- **Download Avoidance**. Never approve anything to be loaded on your computer that was downloaded from an email or website unless you specifically went to a trusted site or made the request. (When in doubt, don't allow it!)
- **Auto Log-Off Setting.** Have your PC automatically time-out and require a password or biometric login to reactivate. Don't leave your computer unattended in an unlocked mode.
- **Keep passwords private**. Don't share passwords or write them down. Pick passwords that are hard to crack, but easy to remember. Change them on a frequent basis.
- **Secure your computer and networks**. Install and maintain firewalls, spam filters, and real-time anti-virus, spyware and malware protection software. Block access to sites that are unnecessary or represent high fraud risk for malware, (online gambling social media, adult entertainment, hacker sites, etc).

- **Limit administrative rights.** Don't let employees install software without prior approval.
- **Block pop-ups.** Surf the Internet carefully.
- **Be on the alert for suspicious emails.** Do not open email attachments or click on links.
- **Note any changes in the performance of your computer.** Dramatic loss of speed, unexpected rebooting, computer locks up, unusual popups, etc.
- **Tokens:** Consider using security tokens, (soft or fob), to offer another level of out-of-wallet authentications which can be required for any funds transfer transaction.
- **Never access Credit Union accounts from public Wi-Fi hotspots.** Airports, coffee shops, etc.
- **Monitor and reconcile accounts daily.** Make sure employees know how and to whom to report suspicious activity at your company and the Credit Union.
- **Take advantage of security options offered by the Credit Union.** Consult with your Credit Union to determine what security settings and options may help minimize your risk and have them activated.
- **Don't wait.** Notify your manager or IT department if you suspect anything is unusual or not right **immediately**. If it is something that affects Quincy Credit Union, call 617-479-5558 so we may assist you with investigating the issue.

2 b. **COMPUTER SECURITY**

Protecting computers and internal networks from unauthorized access is a challenge where the security plan will differ at each business or Member due to their specific computing needs and structure. Layers of security systems and access rights generally will offer greater protection, but every business should develop and implement a security plan that is designed to prevent and mitigate the risk of CATO. Some of the common elements of a security plan would include many of the items listed below.

- **Network Protection Tools.** These items are used to block unauthorized traffic from entering the internal network, checking for virus/malware and reporting suspicious activity.
  - **Firewall** (Blocks unauthorized traffic)
  - **Anti-Virus Program** (identifies potentially malicious programs and quarantines or automatically removes them from the system and set the scans to update and run daily)
  - **Encryption** (makes data on the network unreadable if stolen)
  - **Anti-Spyware/Malware** (related to Anti-Virus detection suite)
  - **Intrusion Detection System** (looks for incoming attacks to immediately block & report them)
- **Isolated Computer you do your banking on.** Sometimes it may be possible to limit a PC to only conduct banking activity and not allowing it connections for general web browsing, email and social networking to reduce the threat of being infected.
- **Screensavers:** This will lock unattended computers and require a password to unlock it.
- **Network Rights:** Services, directories, programs and access is controlled to limit a user to only be able to perform tasks or access data that they have a business need to use.
- **CD Drives & Thumb-drive Deactivations:** Disable drives to prevent any program or files to be uploaded or downloaded from the network or PC to these removable data media.
- **Website, Application & Pop-Up Blocking**. The firewall or activity monitoring system can be sent to block sites or applications that may represent a greater risk for malware or fraud.
- **Secure Email.** If confidential information is sent using email, there are systems that can encrypt the message so it can only be read by the intended recipient.
- **Penetration Test and Vulnerability Scans**. In some cases, a business may have an external consultant test the security of their systems for possible vulnerabilities from the outside or internal workstations.

- **Laptops & Remote Access Security**. Insure that any PC or device that can access the internal network uses a secure connection. Company laptops may consider encrypting the data drives if confidential information is present.
- **Patch Updates**. Enable automatic updates for operating system patches and browsers.

Quincy Credit Union
Corporate Takeover Account Plan

2 c. **ACCOUNT SECURITY**

A key element of the security procedures is the reviewing of activity on your accounts to help detect any unusual, unauthorized or suspicious activity as soon as possible. Statistics show that Members will discover fraud before the Credit Union in over 60% of the cases. Here are some tips on how to help secure your accounts.

- **Review Daily Activity**. Check the account transactions that post on a daily basis to look for anything that is not authorized. . If you used Quicken or QuickBooks, consider downloading transactions daily to keep your accounting records up-to-date and quickly identify anything unusual.
- **Reconcile**: Balance the accounts at least -monthly and report any errors or unauthorized entries promptly
- **Limit Access**: Only allow staff with a need to access or initiate transactions rights to the account. (Review the staff list and access rights occasionally to make sure they are set properly.)
- **Alerts**. Enroll in alerts (text and/or emails) to be sent to the appropriate staff for any activity that may represent a greater risk, such as debit cards, ACH originations, Wire transfers, external transfers, maintenance changes or significant balance changes.
- **Record Security**. Shred old statements, checks or other confidential records with account numbers and access information. Consider e-Statements to minimize paper record or “dumpster driving”.

2 d. **USER SECURITY**

A key element of the security procedures is the reviewing of activity on your accounts to help detect any unusual, unauthorized or suspicious activity as soon as possible. Statistics show that Members will discover fraud before the Credit Union in over 60% of the cases. Here are some tips on how to help secure your accounts.

- **Limit Administrative Rights.** Do not use the administrator user credentials for performing day-today processing.
- **Never Share User IDs/Passwords.** Issue separate IDs for every staff member and make sure the staff does not share or post the password where others can view or use it.
- **Multi-factor Authentication Logins.** Use a Credit Union that employs systems that use multiple ways to confirm the user’s id or authorization, such as Quincy Credit Union.
- **Use Dual Control**. For monetary transactions, require two different users to complete the transaction. One would create the transaction and a different user will be required to approve it before it can be processed.
- **Enroll in Alerts.** Sign up for transaction, debit cards, maintenance and balance alerts to be sent whenever there is activity on the account or user.
- **Keep Contact Information Current.** This is important if the Credit Union needs to contact the user to confirm any suspicious transaction. The cell phone number is very important.
- **Require good passwords and changes.** This is a basic security recommendation for any user.
- **Limit Account Access and Right Reviews.** Only give rights that the user needs to perform their duties.

2 e. **DETECTION and RESPONSE**

Time is money! Nowhere is this truer than with a CATO attack because the sooner the fraud is detected and reported, the greater chance to stop future losses and potentially recover funds that may have been taken. The steps listed in the prior sections will enhance the security procedures that should help stop or detect suspicious of unauthorized activity quickly.

If you suspect or identify an unauthorized transaction has been attempted or completed, **NOTIFY US IMMEDIATELY**! We prefer a telephone call to at (617) 479-5558 and a Call Center Representative will gather information, block user access and get the investigation started. If you feel your PC has been compromised, turn it off or disconnect from the Internet immediately to block further access by the Fraudster. We will work with your Staff to monitor your accounts and determine the source of the security breach.

3. EXPLANATION OF POTENTIAL LIABILITY

Businesses are expected to employ reasonable security procedures when conducting financial transactions. CATO frauds typically target security lapses at the business, access device (PC, email, mobile phone) or user level. In most cases, the Credit Union is not in a position to control or dictate what security policies or procedures are actually used by the business or Member when conduction their banking electronically. As mentioned before, if a loss occurs, the business/Member may be held liable for the portion of the loss that can be attributed to their failure to use reasonable care and security procedures as recommended by the Credit Union. The amount of loss can be sizable and therefore requires that the business take appropriate measures to incorporate the security procedures that are recommended and available as long as they do not result in unreasonable demands on the business or user.

If a CATO loss does occur, the Credit Union will work with our Members to seek the most appropriate resolution to the situation. If the Credit Union fails to perform our fiduciary duties in accordance to industry standards, we generally will assume all or some of the liability. We will follow all applicable laws and regulations when dealing with a CATO incident.

5. OTHER RESOURCES

Below are some resources that may provide other helpful information for your business or staff related to frauds and security.

Quincy Credit Union's Security Page. *Access on our website at:*
http://www.qcu.org/home/about/cip/security_information_center#videos

Phishing: Don't take the bait!

Identity Theft: Protect Yourself!

Internet Fraud: If it sounds too good to be true, it probably is

Social Media: Be Careful Who You Trust

Play it Safe with Portable Devices

Quincy Credit Union's Security Page within Homebanking Platform:

https://www.qcu.org/home/diFiles/skins/default/securityvid/story.html

Kevin Mitnick "Home Internet Security Course"

Federal Trade Commission Federal Government ID Theft Response Guide.
http://www.ftc.gov/bcp/edu/microsites/idtheft/

Federal Trade Commission (FTC) Business Guide for Protecting Data. *(use link below)*
http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business

Secret Service Electronic Crimes Task Force: http://www.secretservice.gov/ectf.shtml

Tools and resources: http://www.csbs.org/ec/cato/Pages/catotools.aspx