Business and Corporate Account Take Over Guide

Security information and awareness to help prevent fraud.

What is Corporate Account Take Over?

Corporate Account Take Over is a growing form of electronic crime where malware or malicious software is used to obtain Online Banking login credentials to corporate or business accounts and fraudulently transfer funds from the accounts.

Phishing or masquerading as a trustworthy entity in an electronic communication or social engineering to gain access to your sensitive information may also be used.

These instances can result in substantial monetary loss for your company that, often, cannot be recovered.

How does this happen?

This type of fraud targets employees of a business who have the ability to initiate funds transfers via Online Banking. The goal is to obtain user name and password information.

This is typically done through email links, website links or pop-up links that install a malware program on the targeted person's computer. The malware will secretly record activity and use a "key-logger" to record the user names and passwords as they are entered when logging into an online banking site.

In some cases, social engineering is used to gain information through calls or emails that impersonate their financial institution. Messaging and phone calls claiming the user must update their account information or confirm a password due to a problem or security alert that appears are often used. *Note: Campus Federal will never ask for your user id or password over the phone or via email.*

EDUCATION & INTERNET RISK AWARENESS

The battle begins with awareness.

- **Think!** Responding to any call or email, first ask yourself, "Does this email or phone call make sense?"
- **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!)
- **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. We recommend using a password manager. Never provide your user ID and password to anybody.
- **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.** Do not allow employees to install software without prior approval.
- **Block pop-ups.** Some pop-ups may contain information that can harm your computer. Surf the Internet carefully.
- **Be on the alert for suspicious emails.** Do not open email attachments or click on links from unfamiliar email addresses.
- **Note any changes in the performance of your computer.** Dramatic loss of speed, unexpected rebooting, computer locks up, unusual popups, etc. are red flags your device may need to be checked by a specialist.
- **Initiate ACH and wire transfer payments under dual control.** One person authorizes the creation of the payment file while a second person authorizes the release of the file.
- **Tokens.** Consider using security tokens (soft or fob) to offer another level of out-of-band authentications which can be required for any funds transfer transaction.
- **Never access Online Banking accounts from public Wi-Fi hotspots.** This includes airports, coffee shops, libraries, 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.** Visit with a Campus Federal Representative 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 immediately if you suspect anything is unusual. If it is something that affects Campus Federal Credit Union,

call 225-769-8841 so we can help you investigate the issue.

COMPUTER SECURITY

Utilize computer and network security.

- **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** This network security device monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- **Security Suites with Anti-Virus Program** This network security device identifies potentially malicious programs and quarantines or automatically removes them from the system and set the scans to update and run daily.
- **Drive encryption** This technology encrypts data stored on a hard drive. Data on an encrypted hard drive cannot be read by anyone who does not have access to the appropriate key or password, making the data unreadable if stolen.
- **Anti-Spyware/Malware** This technology is related to Anti-Virus detection suite.
- **Intrusion Detection System** This technology looks for incoming attacks to immediately block & report them.
- **Isolated Online Banking Computer** If possible, have one PC that is only used conduct online banking activity. To reduce the threat of being infected, no connections for general web browsing, email and social networking should be allowed on this PC.
- **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.
- **Website, Application & Pop-Up Blocking**. The firewall or activity monitoring system can be set 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.

ACCOUNT SECURITY

Review accounts regularly to help detect unusual or fraudulent activity.

- **Review Daily Activity**. Check the account transactions that post on a daily basis to look for anything that is not authorized. If you use 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 and e-Notices to minimize paper record or mail theft.

USER SECURITY

Review user information regularly to help detect unusual or fraudulent activity.

- **Limit Administrative Rights.** Do not use the administrator user credentials for performing day-to-day 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 Campus Federal 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.
- **Use Out-Of-Band Security methods.** Where possible, use an out-of-band method to confirm financial transactions initiated over an electronic channel.

Out-Of-Band means that a confirmation is performed using a different method from how the transaction was created. For example, if a computer was used to create a transaction via an Internet banking site, a cell phone call would be placed to the user to confirm they submitted the transaction.

- **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 strong passwords and require password 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.

DETECTION AND RESPONSE

Time is money! The sooner fraud is detected and reported, the greater chance to recover funds and prevent future losses.

If you suspect or identify an unauthorized transaction has been attempted or completed, notify Campus Federal immediately by calling 225-769-8841 or toll-free 888-769-8841.

USER SECURITY

Campus Federal has incorporated layered security methods into our electronic security services to strengthen the effectiveness of our fraud prevention efforts.

OTHER RESOURCES

- Federal Trade Commission Federal Government ID Theft Response Guide
- Federal Trade Commission (FTC) Business Guide for Protecting Data.
- National Institution of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses
- Fraud Advisory for Business Corporate Account Takeover" joint issued by U.S> Secret Service, FBI, IC3 and the FS-ISAC
- NACHA – The Electronic Payments Association's Resource Center for Corporate Account Takeover