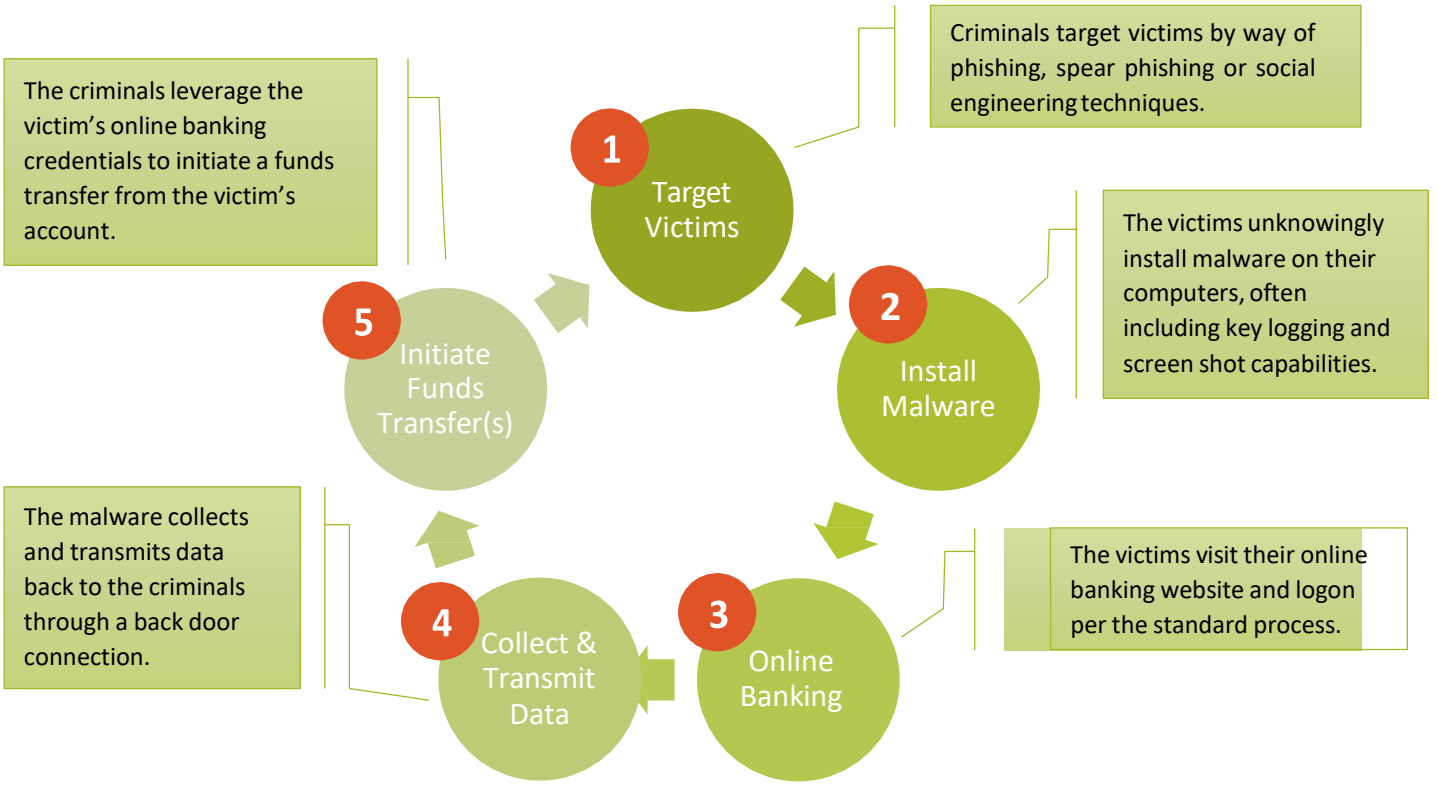
Corporate Account Takeover

Corporate Account Takeover and Online and Data Security Best Practices

Corporate Account Takeover (CATO) is a form of corporate identity theft where a business' online banking credentials are stolen by malware. Criminal entities can then initiate fraudulent banking activity, including wire transfers and ACH payments. CATO involves compromised identity credentials at your, our customer's, place of business or via your mobile devices, not compromises to the wire system, ACH network, or bank systems.

Dissecting a CATO Attack



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).

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. 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:
    - UPS (e.g., "There has been a problem with your shipment.")
    - Financial institutions (e.g., "There is a problem with your banking account.")
    - Better Business Bureaus (e.g., "A complaint has been filed against you.")
    - 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.
- 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.

Online Payment System Security Best Practices

The United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center, and the Financial Services Information Sharing and Analysis Center have developed online security best practices that should be utilized by all commercial customers, including small businesses and sole-proprietors. The full advisory document can be viewed online at http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf, and a summary is provided below.

Protect, Detect and Respond

Protect

1. Educate everyone on this type of fraud scheme.
2. Enhance the security of your computer and networks to protect against this fraud.
3. Enhance the security of your corporate banking processes and protocols.
4. Understand your responsibilities and liabilities.

Detect

1. Monitor and reconcile accounts at least once a day.
2. 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).
3. Note any changes in the performance of your computer.
4. Pay attention to warnings.
5. Be on the alert for rogue emails.
6. Run regular virus and malware scans of your computer's hard drive.

Respond

1. If you detect suspicious activity, immediately cease all online activity and remove any computer systems that may be compromised from the network.
2. Make sure your employees know how and to whom to report suspicious activity to within your company and at your financial institution(s).
3. Immediately contact your financial institution(s).
4. 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.
5. File a police report and provide the facts and circumstances surrounding the loss.
6. Have a contingency plan to recover systems suspected of compromise.
7. Consider whether other company or personal data may have been compromised.
8. Report exposures to PCI DSS if you accept credit card payments.

Other Online and Data Security Best Practices

1. Install a dedicated, actively managed firewall. A firewall limits the potential for unauthorized access to a network and its computers.
2. Install commercial anti-virus software on all computer systems.
3. Ensure virus protection and security software are updated regularly.
4. Ensure computers are patched regularly, particularly operating system and key applications, with security patches.
5. Consider installing spyware detection software.
6. Be suspicious of emails purporting to be from a financial institution, government department or agency, or payment processors (such as PayPal) requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes or similar information. If you are not certain of the source, do not click any links.
7. Be suspicious of pop-up boxes asking you to update your contact information (specifically phone numbers) at any time, even if the pop-up occurs just after you have logged in to online banking.
8. Create strong passwords.
9. Prohibit the use of "shared" usernames and passwords for online banking systems.
10. Use a different password for each website that is accessed.
11. Change the password several times a year.
12. Never share username and password information with third-party providers.
13. Limit administrative rights on users' workstations.

14. Carry out all online banking activities from a stand-alone computer system from which email and web browsing are not possible.
15. Verify use of a secure session (https://) in the browser for all online banking.
16. Avoid using automatic login features that save usernames and passwords for online banking.
17. Never leave a computer unattended while using any online banking or investment service.
18. Never access bank, brokerage or other financial services information via public wifi – for example at hotels, restaurants, public libraries. Unauthorized software may have been installed to trap account number and sign on information leaving you vulnerable to fraud.

Other Online and Data Security Resources

The following is a list of resources that you, as a business owner, can take advantage of to educate yourself and your employees on online and data security.

IC3 – *CATO Fraud Advisory*
http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf

FCC – *Small Business Cyber Planner*
http://www.fcc.gov/cyberplanner

Better Business Bureau – *Data Security Made Simpler*
http://www.bbb.org/data-security/

NACHA – *Corporate Account Takeover What You Need to Know*
https://www.nacha.org/system/files/resources/CAT%20Need%20to%20Know.pdf

This document is for informational purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions, and security threats change constantly.

***Sources** | NACHA, the Financial Services – Information Sharing and Analysis Center, and the Internet Crime Complaint Center.*