

Cyber Fraud Preventing Account Takeovers



Presented by Retired
FBI Special Agent
Jeff Lanza

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. 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.

Source: FBI

How it is Done:

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, sometimes 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. Criminals also may disguise 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.”)

Crooks may also use 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.

Detect

- ✓ **Monitor and reconcile accounts at least once a day.**
- ✓ **Discuss the options offered by your financial institution to help detect or prevent out-of-pattern activity.**

Speaker Information: Jeff Lanza

Phone: 816-853-3929

Email: jefflanza@thelanzagroup.com

Web Site: www.thelanzagroup.com

What You Can Do to Keep Safe - Education

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.
- 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.

What You Can Do to Keep Safe - Computers

Enhance the security of your computer and networks to protect against this fraud.

1. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.
2. 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.
3. 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.
4. Install routers and firewalls to prevent unauthorized access to your computer or network.
5. Change the default passwords on all network devices.
6. Install security updates to operating systems and all applications, as they become available.
7. Block pop-ups.
8. Keep operating systems, browsers, and all other software and hardware up-to-date.
9. 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)