NORTH Dakota | Securities
Be Legendary.

Informed Investor Advisory: Account Takeover Fraud

What is Account Takeover Fraud?

Account takeover (ATO) fraud occurs when a bad actor gains unauthorized entry to an investor's account, which enables them to conduct fraudulent financial transactions. They will often use compromised security information (e.g., logins and passwords) to access bank and brokerage accounts for the purpose of conducting illegal funds transfers, retail purchases, and trading activity.

ATO attacks and their related financial losses are increasing exponentially. The average financial loss from a successful ATO fraud is nearly $12,000 per incident, while approximately 22% of U.S. adults and 24 million households have been victims of some type of ATO. These statistics highlight the prevalence of these types of attacks and the need for investor vigilance.

Good Cyber Habits are Key to Protecting Against ATO Fraud

Bad actors use various online methods to acquire investor information for ATOs including software exploits, phishing emails/text messages, malware, trojan horses, social engineering schemes, and other techniques. The majority of ATO victims reported using the same password for multiple online accounts. Critical steps investors can take to protect themselves against ATOs include:

- **Strong and Frequently Updated Private Passwords** - Investors should have passwords or passphrases that are at least 8 characters long and use a mix of letters, numbers, and special characters. Passwords and passphrases should not be shared and should be changed periodically.

- **Use Multi-Factor Authentication** - Using multiple forms of authentication (e.g., security questions) provides another layer of protection.

- **Antivirus Software** – This type of software can help identify and protect against potential vulnerabilities and malware threats.

- **Update Software** - Make sure your computer has the most recent security patches to protect against vulnerabilities and exploits from cybercriminals.

- **Don't Click on Links or Download Files/Software from Unknown Sources** - Phishing and malware ATO schemes depend on these actions.

- **Confirm Secure Web Connection for Financial Accounts** - When logging into accounts, make sure the website starts with https:// and has a closed padlock on the status bar.

Identifying ATO Fraud: Red Flags

ATO fraud can be difficult to detect, which makes personal monitoring of your financial activity, statements, and messages extremely important for preventing/minimizing financial losses from ATO fraud. Some red flags for identifying potential ATO fraud are:

- **Unfamiliar Transactions** - Financial transactions that you do not recall initiating point to potential ATO fraud.

- **Unexpected Notification of Updated Contact Information** - Cybercriminals often change account addresses and phone numbers to prevent customers from receiving their account information, making it easier to conduct a fraudulent transaction.

- **Unknown Credit Report Accounts** - Bad actors can use information from ATOs to open new accounts and make fraudulent transactions.

- **Chargeback Requests/Fraudulent Transaction Claims** - An unusual number of claims/requests suggests someone may have access to your account(s).

- **Password Resets** - Unauthorized password changes often indicate a potential ATO.

How to Respond to an ATO

ATO fraud can happen to anyone, so it is important to have a plan in place to mitigate the damages from an attack. Here are some actions individuals should take once they learn of an unauthorized intrusion in their account(s):

- **Contact the Investment Firm or Financial Institution** - Individuals should immediately contact their investment firm or financial institution to make them aware of an ATO, so they can attempt to freeze or close the account(s) and limit the damage.

- **Alert Contacts** - Once an ATO occurs, a bad actor may have access to an individual's contacts or business associates and attempt to conduct further criminal actions.

- **Review Financial Activity and Accounts** - Identify what activity is potentially fraudulent on your statements and make sure other financial accounts are not affected.

- **Change Passwords** – Unauthorized access means an individual's account(s) is compromised, so it is a good practice to change your passwords immediately.

- **Check Credit Reports** – Routinely check your credit report to identify potential suspicious activity/fraudulent accounts and seek to have them frozen or closed.

The Bottom Line

ATO fraud is an emerging and growing financial cybersecurity threat that requires investors to be diligent in monitoring their financial accounts and establishing strong cyber habits. By implementing the recommendations in this advisory, investors can prevent and mitigate the negative effects of ATO fraud.