



Contact:
John Yaros
Securities Bureau Chief
(208) 332-8077

NEWS RELEASE

FOR IMMEDIATE RELEASE

April 10, 2023

Account takeover (ATO) fraud is a growing type of cybercrime and financial fraud that individuals can mitigate their exposure to by practicing proper cyber hygiene. Individuals should diligently monitor their financial activity to identify ATOs and contact their financial institutions immediately if fraudulent activity is suspected.

Financial Literacy Tip of the Week Account Takeover Fraud: An Emerging Financial Cybersecurity Risk

Boise, Idaho... The Idaho Department of Finance is encouraging Idahoans to be aware of a growing type of cybercrime and financial fraud known as Account Takeover Fraud, or ATO.

What is Account Takeover Fraud?

ATO fraud occurs when a bad actor gains unauthorized entry to a customer's financial account, which enables them to conduct fraudulent financial transactions. ATO schemes often involve illicit actors using compromised customer information (e.g., logins and passwords) to access bank and brokerage accounts for the purpose of conducting illegitimate 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.¹ These statistics highlight the prevalence of these types of attacks and the need for customer financial vigilance.

Cyber Hygiene is Key to Protecting Against ATO Fraud


In order to perform an ATO, illicit actors usually steal customer information online to gain access to their financial accounts, which makes proper cyber hygiene a useful tool against ATOs. Bad actors use various online methods to acquire customer 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 (see chart to the right).²

Critical steps all individuals can take to protect themselves against ATOs include:



¹ <https://www.security.org/digital-safety/account-takeover-annual-report/>

² <https://seon.io/resources/statistics-account-takeover-fraud/>

- **Strong and Frequently Updated Private Passwords-** Individuals should have passwords that are at least 8 characters long and use a mix of letters, numbers, and special characters. Passwords 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 for individuals from illicit actors.
- **Install Antivirus/Spyware Software-** These types 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.

Potential Red Flags for Identifying ATO Fraud

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.
- 🚩 **Updated Contact Information-** Cybercriminals often change account addresses and phone numbers to separate customers from their account(s) to conduct fraud.
- 🚩 **Unknown Credit Report Accounts-** Illicit 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 Financial Institution-** Individuals should immediately contact their 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-** An unauthorized intrusion means an individual's account(s) is compromised, so it is a good practice to change your passwords immediately.
- **Check Credit Reports-** Identify potential suspicious activity/fraudulent accounts and seek to have them frozen or closed.

In Summary

ATO fraud is an emerging and growing financial cybersecurity threat that requires individuals to be diligent in monitoring their financial accounts and establishing strong cyber hygiene practices. By implementing the recommendations in this statement an individual can prevent and mitigate the negative effects of ATO fraud.

Consumers can obtain information about financial firms, professionals or products, as well as view more Department press releases and other information on the Internet at <http://finance.idaho.gov> or by contacting the Department at (208) 332-8000 or Idaho toll-free at 1-888-346-3378.