Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-112525-PSA
November 25, 2025

Account Takeover Fraud via Impersonation of Financial Institution Support

The FBI warns of cyber criminals impersonating financial institutions to steal money or information in Account Takeover (ATO) fraud schemes. The cyber criminals target individuals, businesses, and organizations of varied sizes and across sectors. In ATO fraud, cyber criminals gain unauthorized access to the targeted online financial institution, payroll, or health savings account, with the goal of stealing money or information for personal gain. Since January 2025, the FBI Internet Crime Complaint Center (IC3) received more than 5,100 complaints reporting ATO fraud, with losses exceeding $262 million.

HOW IT WORKS

The cyber criminal impersonates the financial institution's staff or website, to obtain access to the account. Cyber criminals usually gain access to accounts through social engineering techniques — including texts, calls, and emails — or through fraudulent websites.

Social Engineering

- A cyber criminal manipulates the account owner into giving away their login credentials, including multi-factor authentication (MFA) code or One-Time Passcode (OTP), by impersonating a financial institution employee, customer support, or technical support personnel. The cyber criminal then uses login credentials to log into the legitimate financial institution website and initiate a password reset, ultimately gaining full control of the accounts.

- Social engineering methods include contacting account owners via fraudulent text messages, calls, or emails to trick the email recipient into providing their login credentials. In some instances, the cyber criminal states there are fraudulent transactions on the financial account and may provide a link to a phishing website that the account owner believes will report the fraud or prevent additional fraudulent transactions.

- In some instances, cyber criminals impersonating financial institutions reported to the account owner that their information was used to make fraudulent purchases, including firearms. The cyber criminal convinces the

account owner to provide information to a second cyber criminal impersonating law enforcement, who then convinces the account owner to provide account information.

Phishing Domains/Websites

- The cyber criminal uses a phishing website that looks like the legitimate online financial institution or payroll website to trick the account owner into giving away their login credentials. Believing the phishing website is the legitimate one, users enter their login credentials into the fraudulent site, unknowingly providing them to cyber criminals.
- Cyber criminals may also use a technique called Search Engine Optimization (SEO) poisoning. SEO poisoning refers to cyber criminals purchasing ads that imitate legitimate business ads to increase the prominence of their phishing websites by making them appear more authentic to customers who use a search engine to locate the business' website. When users click on the fraudulent search engine ad, they are directed to a sophisticated fraudulent phishing site that mimics the real website, tricking users into providing their login information.

Once the impersonators have access and control of the accounts, the cyber criminals quickly wire funds to other criminal-controlled accounts, many of which are linked to cryptocurrency wallets; therefore, funds are disbursed quickly and are difficult to trace and recover. In some cases, including nearly all social engineering cases, the cyber criminals change the online account password, locking the owner out of their own financial account(s).

STAY PROTECTED

Stay vigilant against ATO fraud attempts by following these tips.

Be careful about the information you share online or on social media.	***Monitor your financial accounts on a regular basis.***	***Always use unique, complex passwords.***
By openly sharing information like a pet's name, schools you have attended, your date of birth, or information about your family members, you may give scammers the information they need to guess your password or answer your security questions.	Watch for irregularities, such as missing deposits or unauthorized withdrawals, wire transfers, or expenditures.	Enable two-factor authentication or MFA on any account possible. Never disable it.

Use Bookmarks or Favorites for navigating to login websites.

Avoid clicking on Internet search results or advertisements. MFA will not protect you if you land on a fraudulent login page. Carefully examine any email address, URL, or spelling in unsolicited correspondence.

Stay vigilant against phishing attempts.

Be suspicious of unknown "banking" or "company" employees who call you; don't trust caller ID. Hang up, verify the correct number, and call it yourself. Companies generally do not contact you to ask for your username, password, or OTP.

WHAT TO DO IN CASE OF AN ATO INCIDENT

1 Contact Your Financial Institution

Contact your financial institution as soon as fraud is recognized to request a recall or reversal as well as a Hold Harmless Letter or Letter of Indemnity. Requesting a recall and obtaining a Hold Harmless Letter/indemnification documents as quickly as possible may reduce or eliminate your financial losses. Immediately report fraudulent wire transfers to both to your financial institution and to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov.

2 Reset or Revoke Compromised Credentials

Reset all credentials and passwords that may have been exposed during the intrusion, including user and service accounts, compromised certificates, or other "secret" credentials. If you use the compromised password for other online accounts, change your password on those sites too.

3 File a Complaint

File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.

- Identifying information about the cyber criminals including the financial institution impersonated, name, phone number, address, and email address.
- Any websites or software the cyber criminals may have asked you to visit or download.
- Any financial accounts provided or used by the cyber criminals.

- Include the words "Account Takeover" or "SEO poisoning" in the incident description.

4 Notify the Impersonated Company

Notify the company that was impersonated of the method the cyber criminals used to target the account owner. The company may be able to warn others to watch out for the scam and take proactive measures like requesting phishing pages be taken down.

5 Stay Informed

Visit www.ic3.gov for updated Industry Alerts and Public Service Announcements regarding ATO trends, as well as other cyber-enabled fraud schemes.