Social Media Account Hacked?

How to Regain It and Defend Against an ATO (Account Takeover)

BY **CHRISTOPHER SALGADO,**
CEO OF ALL POINTS INVESTIGATIONS, LLC

So, what's an ATO (Account Takeover)? You may not be familiar with the name, but I assure you you're familiar with this attack. Take a look at the below scenario.

A cloudy and rainy evening wraps up a pleasant, clear and sunny day. While this turn of the environment was forecasted, the evening seems to deliver an unchecked starkness that offers a mist of concern presiding over the night. As you pick up on this and gaze out of your home's window, the phone rings.

On the other end of the call is a rather monotone adult female. She asks you if you're taking in clients this evening. Your eyes dart towards the glowing clock in the room. The clock broadcasting a late-night hour is the only light offering visibility into your room this evening. Given the exhausting hour, you begrudgingly accept her request. You ask how you can assist as your head falls back into your reliable and well-aged, comfortable chair.

The caller says she doesn't know who else to turn to. Not an unusual statement, given your decades-long experience in investigations. In fact, you've heard this statement from clients several times throughout your successful tenure. What does grab your attention is her next several statements.

Her lengthy story details a large portion of her adult life. Once successful and highly regarded, now a shattered path of yesteryear accolades. Her immediate loss of $600K becomes dwindled alongside the impact of her family members and friends who've suffered similar fates and more. The salt in the wound is they all fell victim to large financial attacks in her good name. In turn, your new client has become spiritually crippled. Her former bright-eyed outlook on life has been replaced with that of a cynic of mankind. How can people install such animosity against others only to have their victims suffer even more in the form of ongoing fear, resentment and embarrassment? Yet others adopt a final chapter… suicide.

This extreme transformation in your new client wasn't built overnight. This problem began as a pebble but then dramatically grew into an immoveable mountain of despair due to weeks of suffering the underhandedness of the despicable. I'm talking about the dire effects of scammers engaging in account takeovers (ATOs).

So, what did this ATO look like, specifically? Your client relays that months ago, she received a social media message from her cousin. Her cousin is an upper middle-class person. Your client and her cousin speak fairly regularly and have done so on this social media platform several times. Her cousin stated she was in a bit of a pickle due to a banking error. As such, she requested $5,000 from your client. Again, your client's cousin is well-off, so this amount didn't raise any alarms. As such, your client obliged.

As you may be able to guess, the requests didn't stop there. As you also may have guessed – given the context of this article – the request was not from the true cousin; the request came from a scammer. Your client's generosity to her "cousin" allowed her scammer to become more

and more brazen with his greed.

The details of the many subsequent requests for money from the scammer included your client receiving multiple requests from her "cousin" via platform messages, email and even text messages from her cousin's phone. All of these messages successfully bore additional details of her misfortunes as to why she needed to request multiple amounts of money from your client. After a hiccup in your client's own social media account, she began receiving emails from her cousin. These emails offered photos of her cousin holding documents in her hands to confirm that the requests were coming from her. Certainly, in the photos was her cousin.

Nonetheless, the messages weren't from her cousin. Over just a few months, your client sent her "cousin" $600K to support her in her time of need.

Shortly after the last financial replenishment, your client started to realize the scam. She then reached out to her cousin separately. Her cousin reported that none of the sent communications were from her. Her cousin stated that her social media account had been hijacked several weeks ago. She added that she was unable to operate it since then. She also mentioned that her phone number was taken from her via a SIM swapping attack. (SIM swapping is when a scammer dupes your phone carrier to believe the scammer is you; the scammer then requests the carrier to swap out a SIM card for the one possessed by the scammer. The result is your phone number is removed from you and granted to the scammer, rewarding the scammer with almost unchecked, full access to your phone and any accounts tied to that phone number.)

Your client relays that her cousin also stated that she has not been able to use her former phone number for several weeks. When she learned of the loss of her number, she didn't know what else to do but get a new number. Unfortunately, she did not report this to anyone, including her social network. Your client states a lack of communication is not atypical of her cousin.

After learning all this from her cousin, your new client's stomach sunk as she realized she had been swindled out of $600K.

Digging into the matter a bit more, now with the assistance of the true cousin, your client discovered that several of her friends succumbed to similar fates. Some suffered even greater fates due to such large losses that they became ashamed and inherited mental instability.

Remember that hiccup in your client's social media account that was listed above? It turns out that your client's social media account also suffered the fate of an ATO. Unbeknownst to your client, several of her family members and friends were scammed in her name. The details of the additional scams appear eerily too similar to not be related to the same illicit operation.

Unfortunately, the above scenario is far from unusual. Quite the opposite. ATOs are extremely effective attacks against persons. This is because they allow for scams to be generated in the names of trusted persons. ATOs allow for scammers to engage the victim's social network via a trusted channel. You can engage with a friend, family member or peer one day and the next day, suffer an ATO and now your same audience is illicitly being engaged in your name. The trust factor is high in these types of attacks because the communication is coming from "you."

Various reports agree that ATOs are highly concerning and significantly on the rise because they work! ATOs bypass the pathetic faux pas of a phishing scam filled with grammatical errors that mismatch with the known written voice of the supposed sender. Such red flags allow for many of us to escape ill fates by picking up on these errors. ATOs are effective and damaging.

The below stats are offered by Security.org. ["Account Takeover Incidents are Rising: How to Protect Yourself", Jan 02, 2025]

- 29% of people (~27M) have experienced ATOs (increased from 22% in 2021).
- 53% of ATOs engaged social media accounts.
- 40% of ATO victims also experienced identity theft afterwards.

Additionally, the same report relays that more current numbers cite 29% of American adults (~20M) having suffered from ATOs. About 20% of victims said the ATO attacks occurred in the last year.

Also noteworthy on this subject is Proofpoint's LinkedIn post on March 10, 2025: "In 2024, 99% of all Proofpoint customer tenants monitored were targeted for ATO."

A report ("Beyond the Breach: Account Takeover Data & Insights) powered by FIBR (Fraud Industry Benchmarking Resource)") published in September 2024 on Sift.com states "In 2023 alone, account takeover fraud resulted in nearly $13 billion in losses, up from $11 billion in 2022.") The same reports tell of a "354% year-over-year increase in Q2 2023."

So how are scammers able to institute an ATO? Honestly, pick your social engineering poison because they come in the form of one or more attacks, such as phishing, SIM swapping (or SIM hijacking), malware and keyloggers, account recovery manipulation, smishing, vishing and the more modern attack vector of quishing. They can also infiltrate your accounts via credential stuffing, brute force attacks or exploitation of leaked data.

Once scammers access your account, they immediately change the password as well as both the reset email and phone number, effectively locking you out of your account. In the event that you've assigned 2FA to your account in the form of an SMS text validation process, a scammer engaging in SIM swapping can easily overcome that.

Once a scammer is in your account, they can initiate their feeding frenzy on your data and/or finances, depending on the account type accessed. Concluding their victimization of you, they can perpetuate the same scam, or another, across your social network. Of course, this approach can include family members, friends and peers. Again, an ATO comes under the guise of legitimacy because your network believes the scammer is you. The scammer can also sell your information to others, but the danger doesn't end there.

More devious scammers can heighten the aggressiveness of their attack against you. This can be done by rolling out a disinformation

campaign against you through posts of "yours" that offend others or positions you in a negative light, including posts that confess engagement in illegal actions, such as CSAM activities. Given that these posts come from your account, they appear to come from you directly, which can result in very concerning situations and repercussions.

So, how do you negate an ATO as much as possible? As regular readers of my articles know, there's no assurance to avoid all scams. That certainly includes ATOs. However, there are several steps to take to possibly avoid these ill fates.

1. Enable two-factor authentication (2FA) on your accounts.
2. Enable multi-factor authentication (MFA) on your accounts.
3. Be cautious of phishing messages. Always verify the authenticity of any communication, especially those requesting personal information or verification codes.
4. Never share your verification code with anyone.
5. Secure your phone number. Use a secure password with your mobile carrier account to prevent SIM-swapping.
6. Monitor account activity. If you notice any suspicious activity or device on your account, immediately log all devices out of your affected account and immediately change your password to that account. If possible, change the password using a new or different device.
7. Avoid recycling passwords. Do not use the same password across different platforms. Some reports indicate ~70% of victims do not adopt unique passwords, which allows them to lose multiple accounts from a single ATO attack.
8. Incorporate hardware-based 2FA on your accounts, such as a YubiKey. The most secure method of 2FA can be utilizing a hardware key, as they cannot be easily intercepted or spoofed like SMS-based verification codes.
9. Keep tabs on your data. Should your information be involved in a breach, change your passwords to all affected accounts.

Implementing the above precautions can heighten your security operations and help you avoid an ATO.

Lastly, should you find yourself the victim of an ATO or should you find another in need of recovery from an ATO attack, it is best to follow the specific platform's recovery process to try to regain your account. If it works, great! Unfortunately, many times, this is unsuccessful. Being a former investigator at Facebook, my firm has assisted in the recovery of accounts across social media platforms. Recovery of email accounts is also possible. Feel free to reach out, should you or another you know have any questions or need any support in this matter.

In the meantime, perhaps us societal do-gooders can assemble together with our powerful prevention education and other resources and redefine ATO from Account Takeover to Anchor of Thwarted Onlinecrime! Assemble, Absolute Terminators of Outlaws! (There's another one for you.) Assemble and stay vigilant! **PI**

Christopher Salgado is a former investigator at Facebook and is CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving Fortune-listed corporations, including a Fortune 20 corporation, law firms and other entities. He is an expert cyber, OSINT and physical investigator as well as an expert social engineer for more than 20 years. His focus includes various categories of threat management, including corporate risk, brand protection, cults, cyberstalkers, supply chain issues, SIU investigations and more. In November 2024, Christopher was named a Top Investigator of 2024 by PI Magazine. He is also a member of the London Speaker Bureau. Christopher has presented on cyber and physical investigations to various companies, law firms and law enforcement agencies, including the FBI, Homeland Security Investigations, ICE, Customs and Border Protection and the DEA as well as members of Interpol, Europol and the European Commission. Christopher was a keynote speaker at CrimeCon 2022 where he spoke on romance scams. He is Founder of Anti-Hackathon (www.AntiHackathon.com), an educational event teaching the public how to be safe online. Christopher is also Founder of AGGOSO™ Training, a comprehensive OSINT training program for investigators, corporations, law firms, journalists and those desiring to upskill their OSINT/cyber investigative skillset. Any questions or comments? Contact him at csalgado@allpointsinv.com. Thank you for reading!