SEON

EBOOK

Account Takeover Attacks: All You Need to Know and How to Stop Them

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

Table of Content

1. Defining Account Takeover (ATO) and ATO Fraud **3**

2. How ATOs Happen **4**

3. Scenario 1: ATO + Scams **5**

4. Scenario 2: ATO + Buying Goods and Services **6**

5. Scenario 3: ATO + Mining for Personal Data **7**

6. Scenario 4: ATO + Reselling Login Details **7**

7. How To Prevent Account Takeover Fraud **8**

7.1 Ensure You Have A Secure Service 8

7.2 Educate Users About the Risks 8

7.3 Deploy Proper Login Monitoring Tools 10

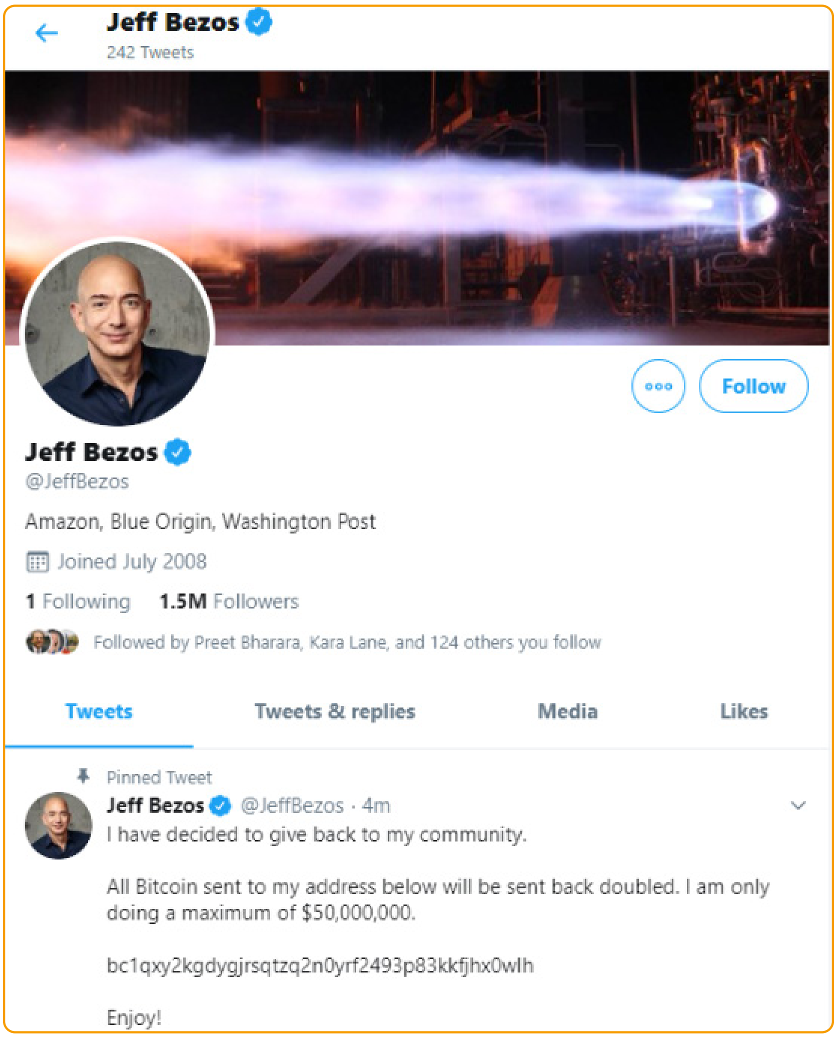
8. Analyse User Behaviour With Velocity Rules **11**

9. Leverage Dynamic Friction **12**

10. Key Takeaway: Protect User and Employee Accounts to Secure Your Business **12**

The news cycle runs so fast these days, it's easy to forget that 2020 saw one of the biggest account takeover attacks in living memory.

We're talking about the July 15 Twitter hack, which saw high-profile accounts such as Elon Musk, Bill Gates, Joe Biden and Jeff Bezos tweet about bitcoin scams.



Jeff Bezos
@JeffBezos

Amazon, Blue Origin, Washington Post

Joined July 2008

1 Following 1.5M Followers

Followed by Preet Bharara, Kara Lane, and 124 others you follow

Jeff Bezos @JeffBezos · 4m
I have decided to give back to my community.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $50,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

But it wasn't just embarrassing for the social media platform and its CEO, Jack Dorsey (whose account was also taken over). It **caused a complete security overhaul at the company**, highlighting some critical system failures at every level.

The question is: **if one of the biggest tech companies in the world can fall victim to an ATO attack, what about yours?** And how should you protect yourself against future attacks? In this guide, we'll attempt to give you some clear tips and tricks, both in terms of educating people at your company, your users and on how to deploy the best anti-fraud tools for better login monitoring.

1. Defining Account Takeover (ATO) and ATO Fraud

An account takeover happens anytime someone logs into someone else's account. For the layman, it will often be referred to as **a hacked account.**

Account takeover fraud happens anytime the person who accesses the account tries to:

- Use the account to scam others (as in our opening example),
- Buys goods or services using the account,
- Mine the account for personal data,
- Sell the account login details.

We'll break down these four scenarios into more detail below, but first, let's see how ATOs happen in the first place.

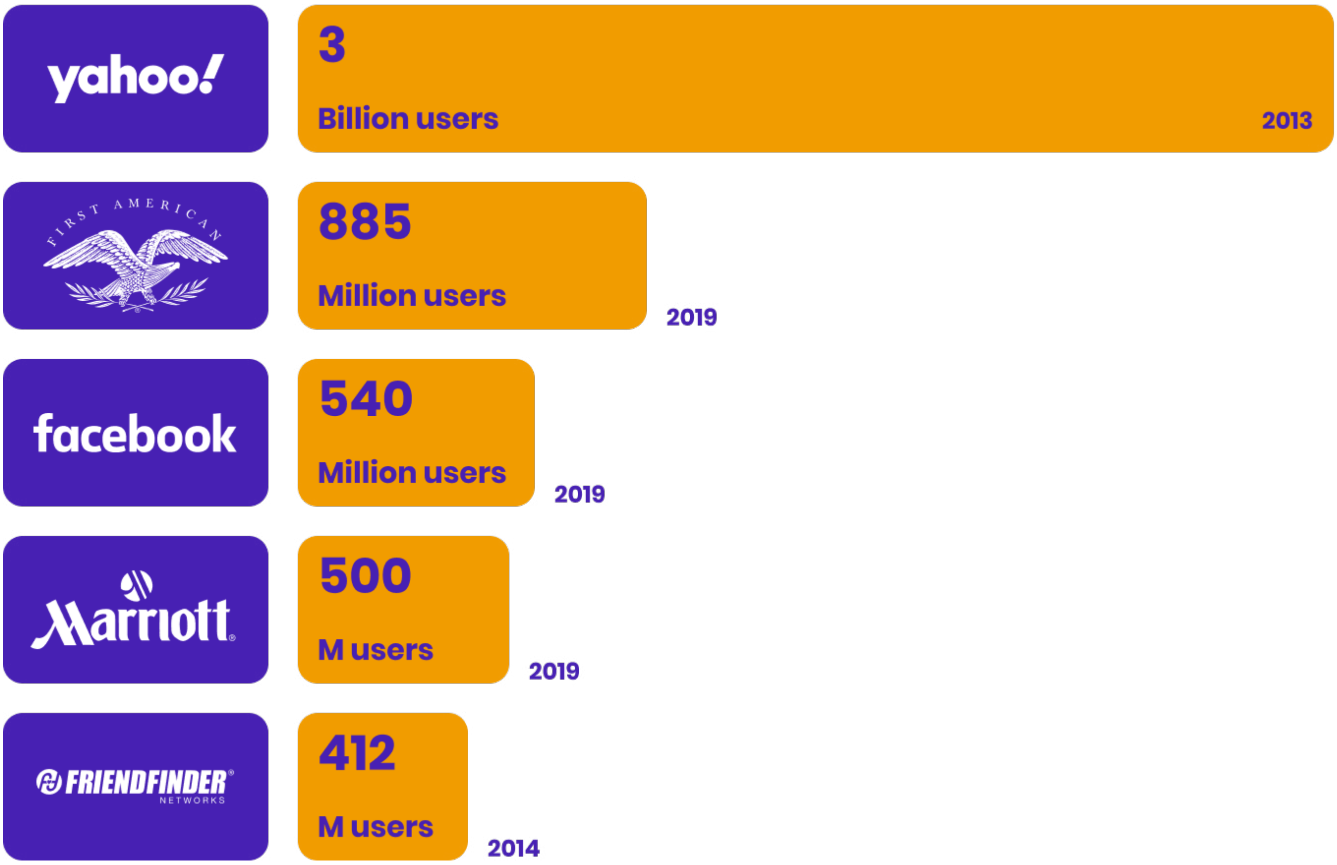
2. How ATOs Happen

There are many paths to a successful ATO.

Opportunistic: a fraudster stumbles upon someone's login details. This could be accidental, or sophisticated, for example following a mass phishing email campaign. It could be because of an easy-to-guess password, brute force, or via malware such as a keylogger.

Bought credentials: Every huge data breach you hear about means a proliferation of ATO attempts is sure to follow suit. This is because these accounts are sold in bulk for cheap on the darknet.

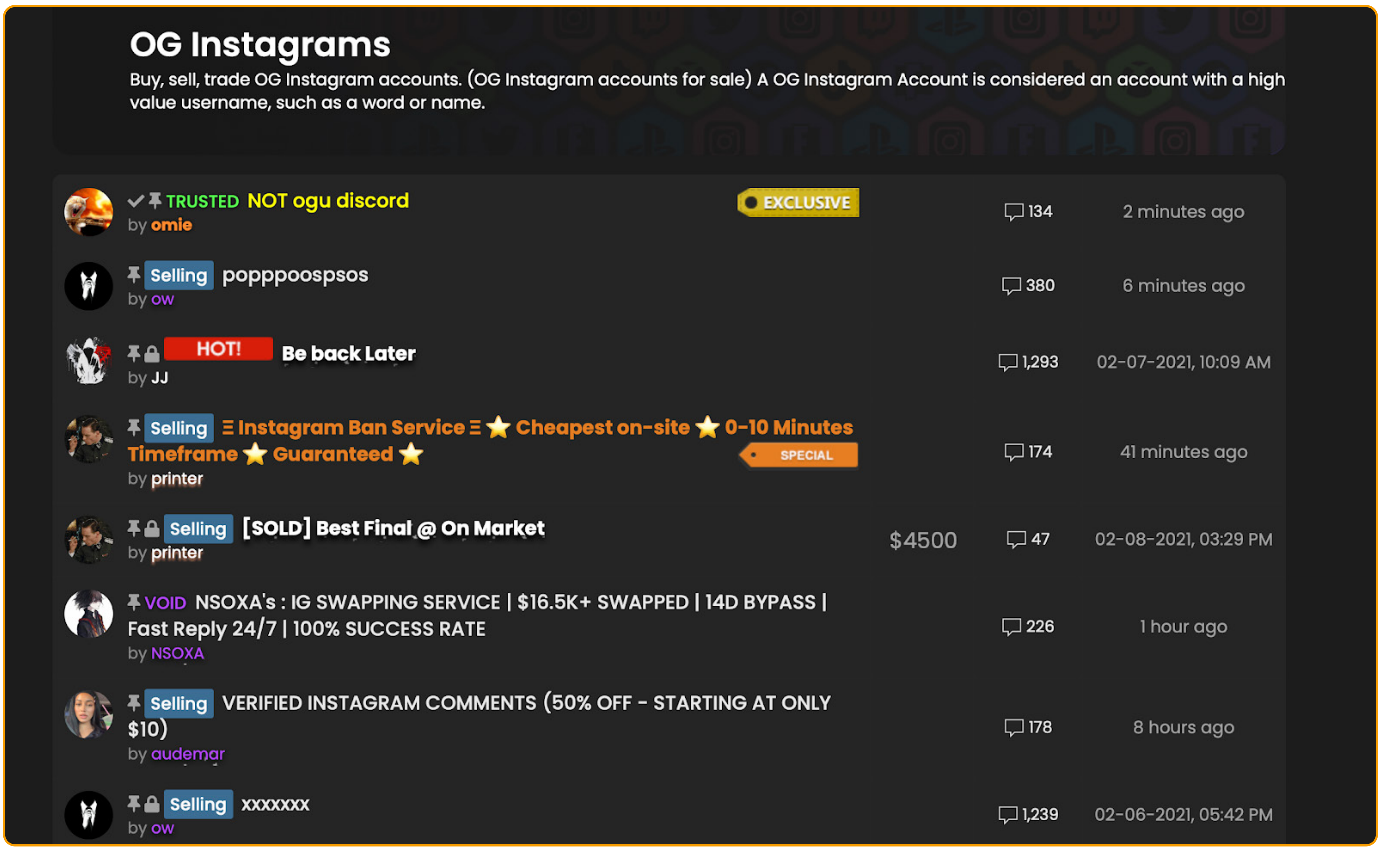
The 5 Biggest data breaches of all time



Credential stuffing: this is when fraudsters automate attacks (usually with bots), to try all the login details they bought on a leaked database.

Exploiting security vulnerabilities: There are a few technical steps you should take to patch holes in your security, such as looking at XSS and SSRF vulnerabilities.

> **Targeted attack:** fraudsters will often target specific accounts which they know to be valuable. In social media and gaming, for instance, there is a huge market of what is known as OG accounts, or accounts with a rare, short handle. To target these accounts, fraudsters often rely on spear phishing techniques (targeted phishing), or SIM-Swapping attacks.



OG Instagrams

Buy, sell, trade OG Instagram accounts. (OG Instagram accounts for sale) A OG Instagram Account is considered an account with a high value username, such as a word or name.

✓ TRUSTED NOT ogu discord EXCLUSIVE by omie		134	2 minutes ago
Selling popppoospsos by ow		380	6 minutes ago
HOT! Be back Later by JJ		1,293	02-07-2021, 10:09 AM
Selling Ξ Instagram Ban Service Ξ ⭐ Cheapest on-site ⭐ 0-10 Minutes Timeframe ⭐ Guaranteed ⭐ SPECIAL by printer		174	41 minutes ago
Selling [SOLD] Best Final @ On Market by printer	$4500	47	02-08-2021, 03:29 PM
VOID NSOXA's : IG SWAPPING SERVICE | $16.5K+ SWAPPED | 14D BYPASS | Fast Reply 24/7 | 100% SUCCESS RATE by NSOXA		226	1 hour ago
Selling VERIFIED INSTAGRAM COMMENTS (50% OFF - STARTING AT ONLY $10) by audemar		178	8 hours ago
Selling xxxxxxx by ow		1,239	02-06-2021, 05:42 PM

A clearnet marketplace for Instagram OG accounts

3. Scenario 1: ATO + Scams

The teenager who managed to take over Twitter accounts from the biggest names on the planet allegedly netted $117,000 in BTC.

Even if the attack was sophisticated, the scam itself was pretty rudimentary: tweet a wallet address and ask people for money.

Things could have been much worse. Being in control of Joe Biden's Twitter account, the fraudster could have attempted to phish personal information from high-security accounts and caused devastating chaos.

Moreover, it was immediately apparent that something wasn't right, which might have helped with damage control.

So in a way, scams that are run from stolen accounts are some of the easiest to manage. But it doesn't mean there aren't any negative consequences for your business.

Consequences for your business: loss of business reputation, customer insult rate goes up, IT resources lost to recovering accounts.

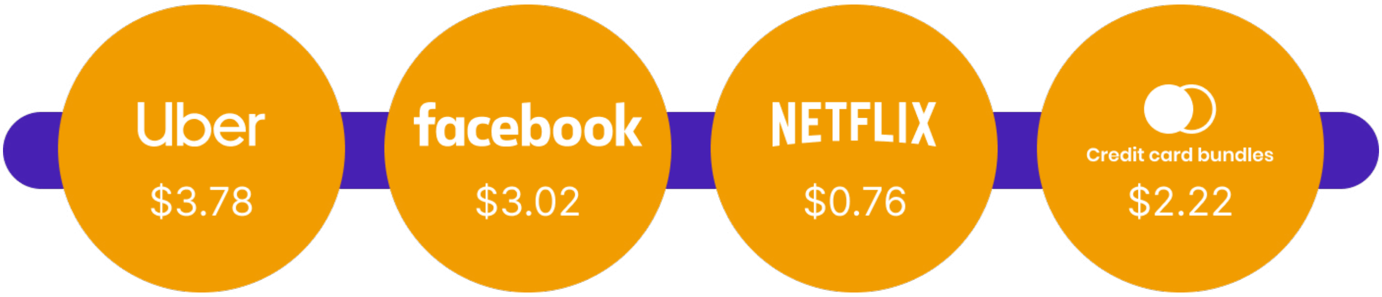
4. Scenario 2: ATO + Buying Goods and Services

If you operate as a digital wallet, losing an account opens a whole new can of worms. First of all, it already means you are a much more valuable target for fraudsters, and that you have a lot more to lose.

We're talking of course about the costs of chargebacks, which not only incur admin fees but can even put you on a high-risk list from card networks, with added transaction fees. This is potentially a death knell for businesses with low margins.

On the bright side, this kind of ATO attack is easier to stop at the withdrawal or transaction stage, for example by identifying a suspicious shipping address or spotting a change of IP address that points to VPN use.

Consequences for your business: high chargeback rates, put on high-risk lists by card networks, reputation damage, higher transaction costs, IT resources lost to recovering accounts.



The value of stolen accounts on the dark web, as reported by TrendMicro

5. Scenario 3: ATO + Mining for Personal Data

The more sophisticated fraudsters will understand how to extract more value from an account by mining it for personal data. They will know how to reset 2FA security for other accounts, or how to download previously submitted KYC documents.

This kind of fraud is much more damaging because it can remain invisible for a long time. And it also snowballs into more fraud down the line, because the personal information will end up as Synthetic ID on other sites.

Consequences for your business: become patient 0 for all kinds of other fraud attacks, reputation loss, in some cases potentially linked to data protection fines, IT resources lost to recovering accounts.

Account Takeover Fraud Vs Identity Fraud

So if someone logs into someone else's account, is it considered identity theft? Technically, no. However, account takeover makes it a lot easier for fraudsters to steal information related to someone's identity. When that data is used to, say, start an online loan application, it does constitute identity fraud – and you're partially responsible.

6. Scenario 4: ATO + Reselling Login Details

Another challenging scenario arises when fraudsters manage to log into an account, and simply resell the details to other unscrupulous individuals.

In that case, the ATO may appear dormant for a long time, until one of the 3 aforementioned actions is performed. Moreover, if accounts from your site end up on marketplaces, their value may go up in the eyes of other fraudsters.

You can read more about the problem in our post on how fraud marketplaces fuel account takeovers.

Consequences for your business: become a higher target for fraudsters, reputation loss, IT resources lost to recovering accounts.

7. How To Prevent Account Takeover Fraud

As we've seen above, one of the worst things about account takeovers is that they open the door to many fraudulent possibilities. The good news, however, is that a combination of education and powerful anti-fraud tools should help you with effective login monitoring.

7.1 Ensure You Have A Secure Service

Starting with the basics, it's all about good online hygiene and ensuring your site is secure. Here are a few examples of things to consider:

- **Follow the best data protection practices:** this is for data that is collected, transferred, processed, and accessed from your site.

- **Use SSL**: especially on pages that collect sensitive information such as credit cards, social security numbers, or addresses.

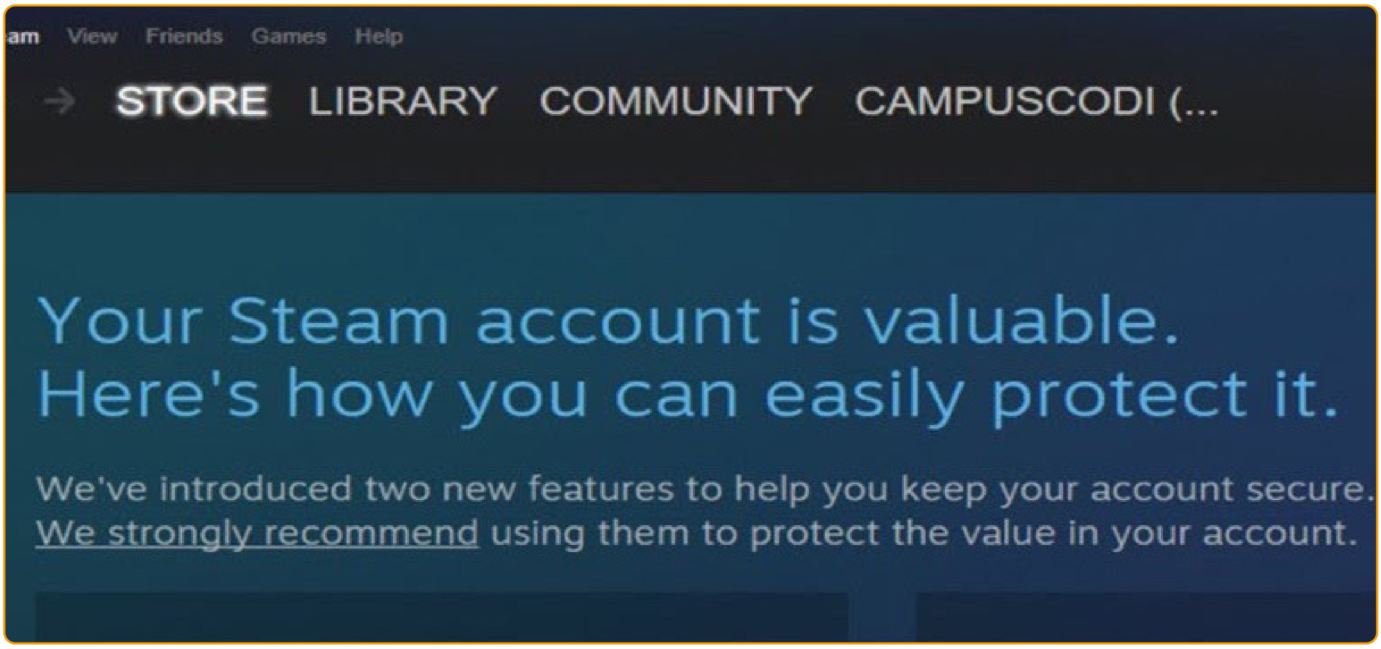
- **Encrypt if possible:** this is just as important for data that's sent via staff members and employees as customer data.

- **Physical device security:** particularly valuable for company phones, laptops and desktop computers. Here again, it's something Twitter did to mitigate future risk by distributing physical security keys.

For companies with extra cybersecurity resources, you could even consider **hiring white hat hackers.** For instance, Facebook has a bug bounty that rewards independent researchers up to $40,000 for finding vulnerabilities that could result in an account takeover.

7.2 Educate Users About the Risks

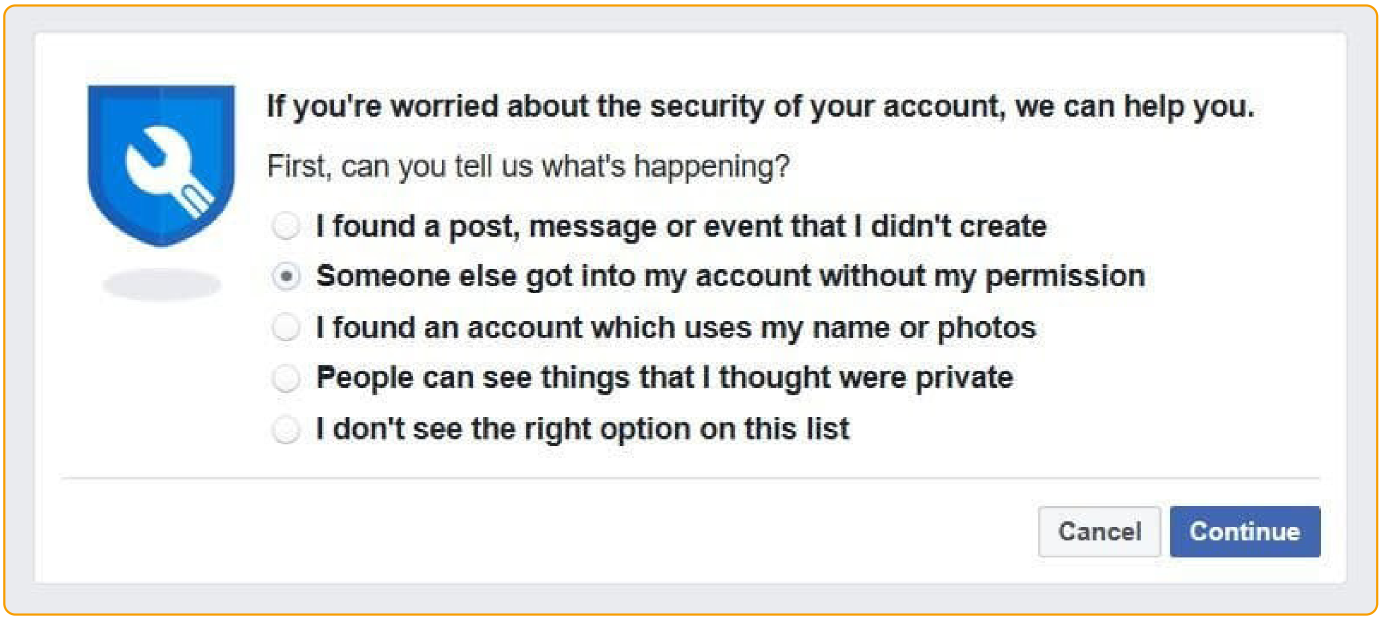
Another good way to boost account takeover fraud prevention: let your users know it's a threat. This is done via regular security notifications, encouraging 2FA authentication, and highlighting the value of their accounts.



Your Steam account is valuable.
Here's how you can easily protect it.

We've introduced two new features to help you keep your account secure.
We strongly recommend using them to protect the value in your account.

How games marketplace Steam encourages 2FA use



If you're worried about the security of your account, we can help you.

First, can you tell us what's happening?

- ○ I found a post, message or event that I didn't create
- ● Someone else got into my account without my permission
- ○ I found an account which uses my name or photos
- ○ People can see things that I thought were private
- ○ I don't see the right option on this list

Facebook's ATO reporting feature

Remember that the sooner you detect an ATO, the sooner you can go into damage control mode and isolate the fraudsters before they cause long term harm.

7.3 Deploy Proper Login Monitoring Tools

However your business operates, the first step to preventing ATOs is to monitor the login stage. Put simply, it's all about **collecting user data any time there is a login attempt, be it successful or denied.**

At that touchpoint, you should be able to detect an IP address, device information, and basic customer behaviour using the following tools:

Device fingerprinting: SEON uses device fingerprinting to create hash/ID using data from a browser, operating system, device and network. This is something that doesn't require excessive calculations, yet can be highly effective in preventing the users from logging in with unknown devices, browsers or devices. It will also detect the use of suspicious emulators or virtual machines, which fraudsters use to multiply attempts from the same device.

IP analysis: A common fraud prevention method that can work great by revealing geolocation, but also suspicious proxies, blacklisted servers, VPNs and TOR usage.

These two powerful tools become even more adept at highlighting suspicious usage when you look at how many attempts stemmed from the same device + IP, or different devices with the same IP.

How suspicious should you be of failed login attempts?

High

Different locations, different devices = high risk. You may be looking at credential stuffing.

Medium

Same location, different devices = medium risk. The user might have forgotten their password and tried to log in from a phone and a laptop.

Low

Different locations, same device = low risk. The user could be travelling.

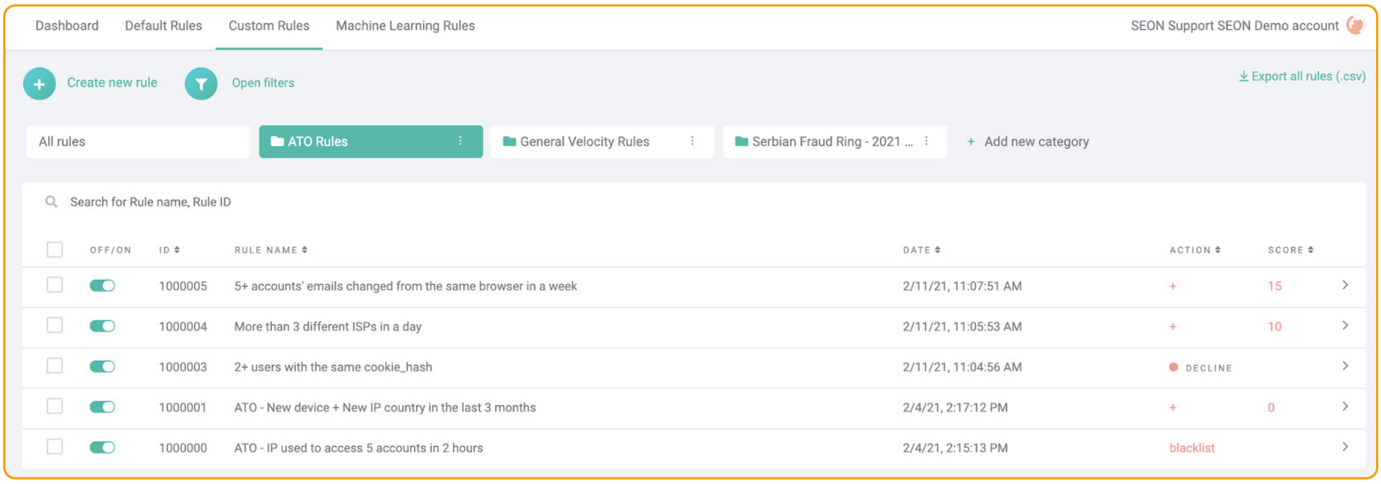
8. Analyse User Behaviour With Velocity Rules

If the fraudster has performed a successful ATO without triggering any alarm bells, you can still spot suspicious activity. This would be done by looking at every user action and assigning them a risk score.

With SEON, this is done **via velocity rules, or user behaviour rules**, which are designed to score anything, from a suspicious address change to adding a combination of high-value items in their checkout.

The beauty of these rules is that you have complete customisation control over which data point is analysed, so you could look at known ATO behaviour such as:

- Unusual number of chargeback requests
- Mass password reset requests
- Shipping address changes
- Very large purchases
- Multiple changes to an account in one session
- Transfers of a large number of reward points
- Keystroke velocity



□	OFF/ON	ID	RULE NAME	DATE	ACTION	SCORE
□	●	1000005	5+ accounts' emails changed from the same browser in a week	2/11/21, 11:07:51 AM	+	15
□	●	1000004	More than 3 different ISPs in a day	2/11/21, 11:05:53 AM	+	10
□	●	1000003	2+ users with the same cookie_hash	2/11/21, 11:04:56 AM	● DECLINE	
□	●	1000001	ATO - New device + New IP country in the last 3 months	2/4/21, 2:17:12 PM	+	0
□	●	1000000	ATO - IP used to access 5 accounts in 2 hours	2/4/21, 2:15:13 PM	blacklist	

Custom ATO Rules in our system

But you can also tailor rules that are very specific to your business. For instance, an online store may have a list of products that are considered high-risk, even if they're not high value. Last but not least, by labelling each case where your fraud prevention system caught an ATO and where it didn't, you could use machine-learning to suggest rules that might not be obvious to the human eye.

9. Leverage Dynamic Friction

One of the key challenges in preventing account takeover is that it's a balancing act with user friction. You don't want security systems that are so stringent that they frustrated your users, especially for something that should be as straightforward as logging in.

The good news? You can use risk scores and set thresholds that will automatically allow login, block it, or require extra verification.

For instance, you could choose to only trigger CAPTCHA verification only after a couple of failed login attempts. Similarly, you could set up rules to allow IP changes if you know your customers are frequent travellers.

The key is to avoid false positives/customer insult rate and to allow legitimate logins to be as easy as possible.

One quick note: if you rely on geolocation to score risk, should have a system in place for users and employees to let you know of a future IP change (for instance when travelling).

10. Key Takeaway: Protect User and Employee Accounts to Secure Your Business

The sad truth is that **there is no company on earth which isn't a target to fraudsters.** It doesn't matter which vertical you're in, how successful you are, or how you do business. If you have user or employee accounts of any sort, someone will try to steal them.

And while it may seem daunting to set up account takeover fraud prevention measures, it does pay in the long term. Nobody will reward you for having a safe system, but customers, partners and investors will certainly hear about it when something goes wrong.

Hopefully, this guide is a good primer on how to set up simple and complex systems to protect your accounts – and your company's reputation.

SEON

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900