SEON

Guide

Reducing Account Takeover Attacks (ATO)

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

Table of Contents

Having trouble protecting your user accounts? Here's your complete guide to understanding and preventing account takeover (ATO) attacks.

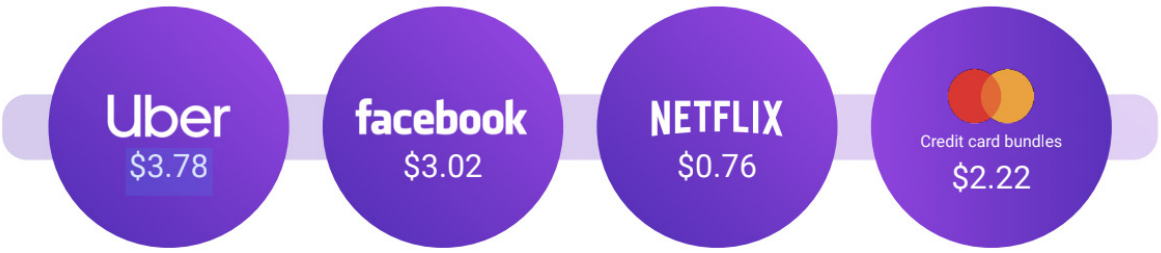
Part 1: Understanding ATO Attacks

Mark Zuckerberg. Elon Musk. Kim Kardashian. Jeff Bezos. Barack Obama. Jack Dorsey. Kanye West.

These are just a few of the names of people whose online accounts have been hacked by fraudsters.

If it can happen to some of the highest-profile people on earth, what about your users? Sure, it may not sound as impressive, but these accounts are just as valuable.

In this guide, we'll see why these accounts are targeted, how fraudsters acquire them, and, of course, which steps you should take to secure them.



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

The Scale of the Problem

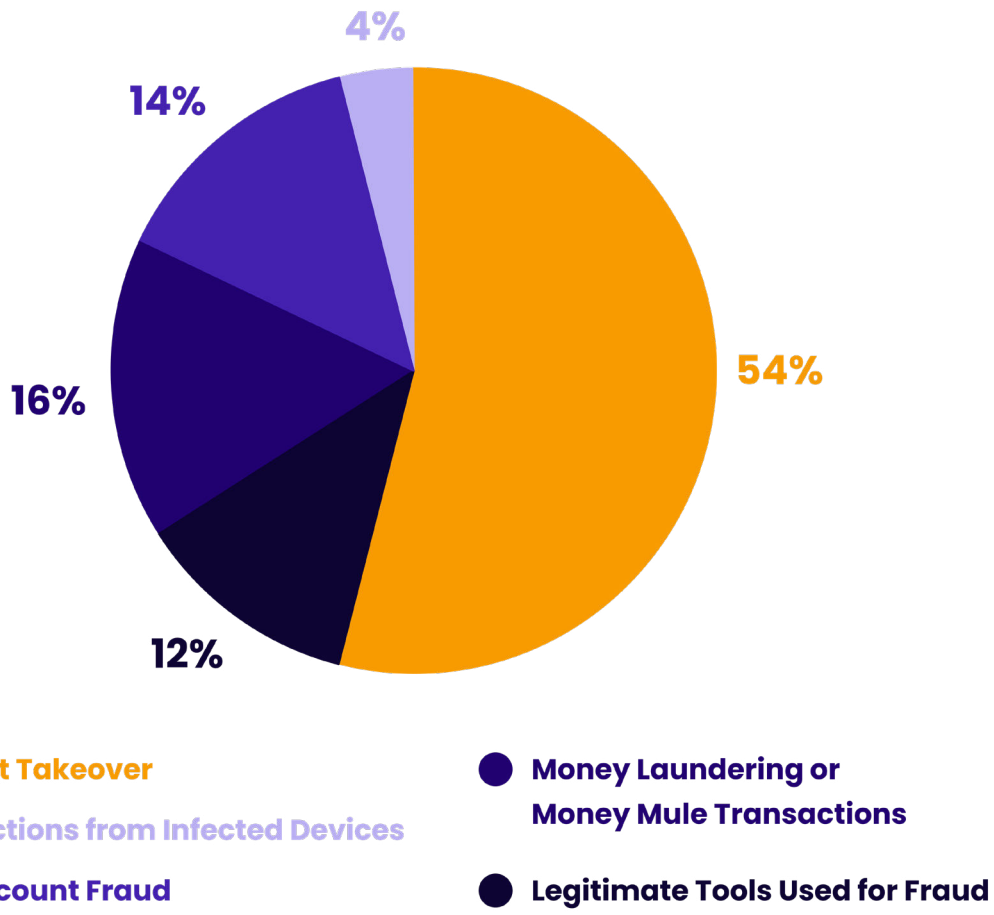
According to research from Kaspersky, more than half of all fraudulent attacks is in fact an account takeover.

While it's harder for businesses to put a monetary value on ATO losses than, say, credit card fraud, it doesn't mean it's a victimless crime.

There are very real consequences for businesses:

- **Hacks and security issues** put a strain on your IT team
- **Support is overwhelmed** by customer requests who attempt to reclaim their account
- The finance department must **fight chargebacks**
- Users turn to competitors due to a **loss of reputation and brand trust**

In the worst-case scenario, stocks can even plummet after a publicised breach (down to 7.5% according to Bitglass research).



8 Reasons Why Account Takeovers Happen

Fraudsters have plenty of reasons to target preexisting accounts:

To acquire more data: Once hackers have entered an account, they can rummage for more information. Is there a phone number attached? Better yet, a valid credit card number? Sometimes, it's about collecting personally-identifying information (PII) for other forms of fraud and identity theft. These types of attacks often target healthcare, the public sector, and even academic institutions.

Financial fraud: all ATOs are designed to extract monetary value at some point down the line. The closest an account is to a credit card, withdrawing funds and wiring money, the better for fraudsters. This is true both for standard currencies, cryptocurrencies, and even loyalty points or gift card credit.

Virtual currency fraud: some currencies are also purely virtual, such as in-game digital items that can be resold for real-world gains.

Promo abuse: Fraudsters rely on multi-accounting techniques to gain as many sign-up or referral bonuses as possible. It's even easier with legitimate accounts they've compromised.

Card testing: certain accounts are only used to make small purchases, or to test credit cards. This helps fraudsters check the validity of stolen credit cards, which can then fuels their criminal buying sprees.

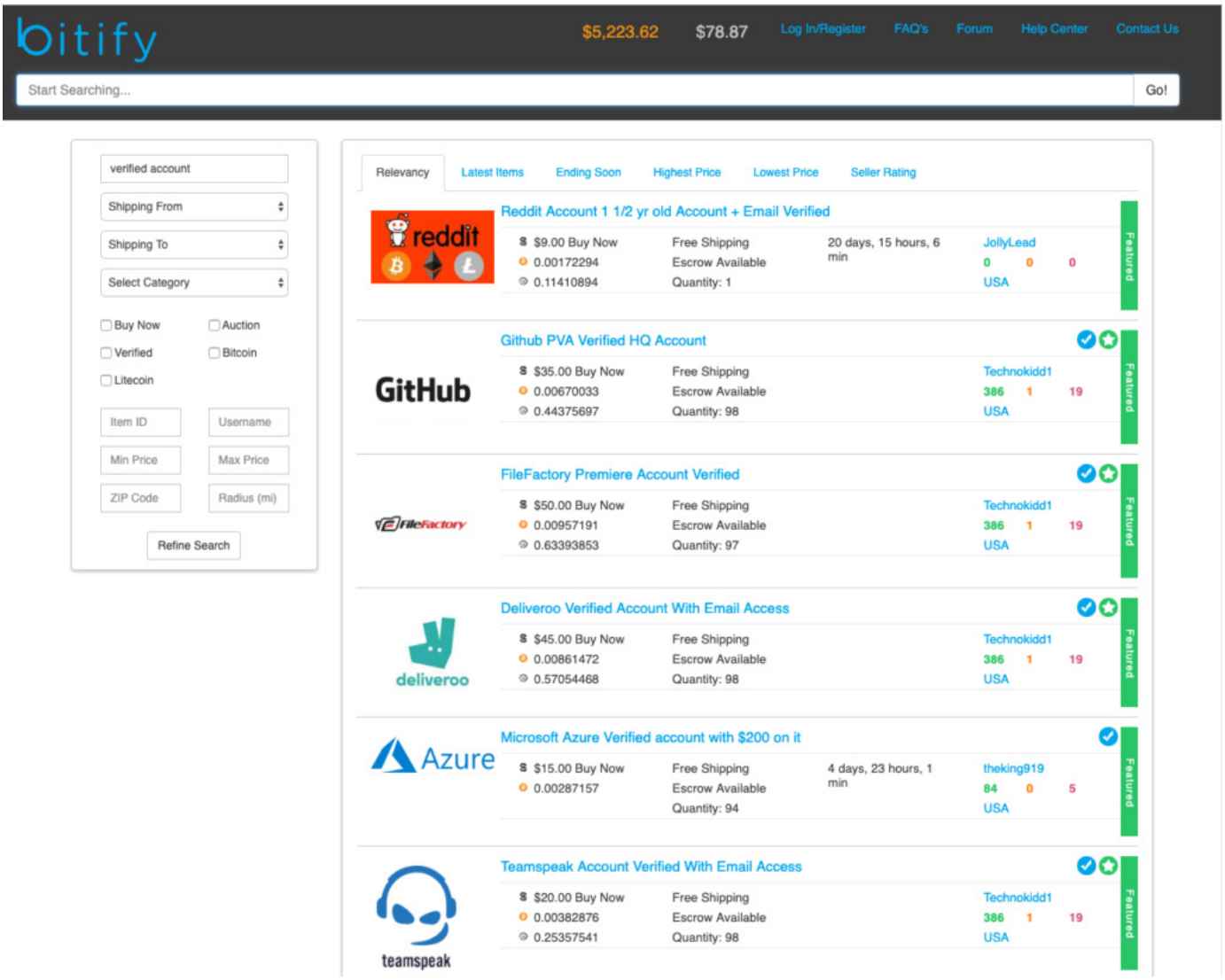
Spam: a legitimate account is a great tool to create fake listings, sell goods that don't exist, write reviews and give feedback on services that are self-serving.

Phishing: Attackers access the account's contacts and target them. The initial account gives them legitimacy and makes the contacts more susceptible to giving away valuable information. A malicious email received from a known contact is more likely to make it past your inbox's spam filter.

Ransom attacks: if an account is extremely valuable, criminals can try to sell it back for a price.

Finally, there is the huge problem of **account reselling**: bad actors lump numerous accounts together and resell them on criminal marketplaces.

This is why account takeover is one of the most damaging fraud attacks in the long run. ATOs fuel fraud marketplaces, which leads to more ATOs.



Example of full accounts available on a clear net site

Data Breaches and Fraud Marketplaces

Criminals have access to a growing number of marketplaces to purchase, sell, and exchange account details.

While the dark web famously provides cover of anonymity, it's now also increasingly easy to buy accounts on clearnet cryptocurrency auction sites or even Telegram groups.

The problem? Every new data breach fuels these marketplaces.

Sadly, in spite of their best cybersecurity efforts, organisations of all sizes are still losing customer records by the millions – a sign that you can't count on standard It security to protect your accounts.

6 Common Account Takeover Scenarios

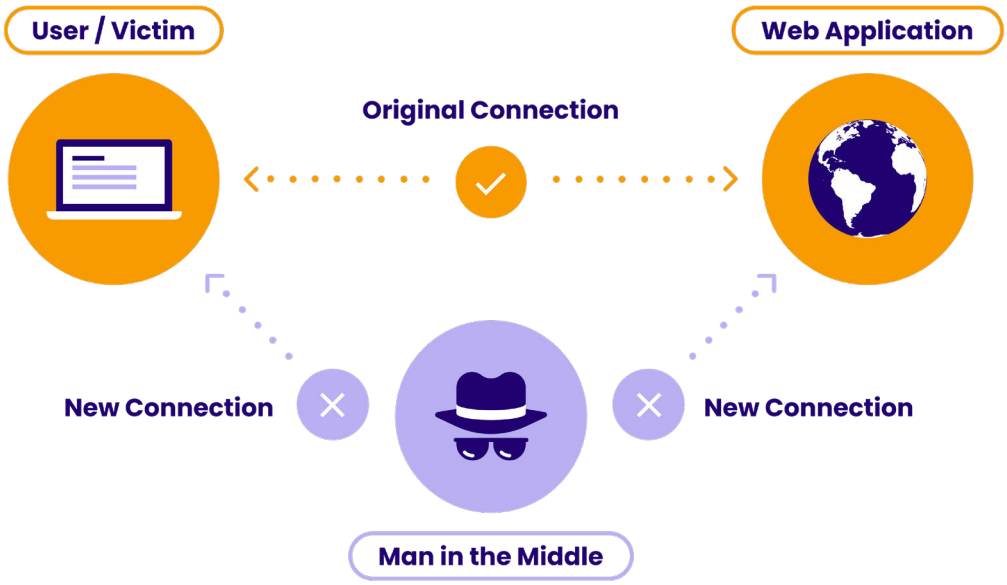
There is no shortage of options for criminals who want to acquire user accounts. Here is a quick overview of the most common methods.

Credential stuffing attack: fraudsters try all the combinations of passwords and email addresses they found in data dumps.

ATO from phishing: criminals send an SMS asking you to log into a clone of a known website. They redirect you to a page where a keylogger captures your password. Options abound for creative criminals here.

Social engineering: fraudsters contact people in person and attempt to extract login info. This works for users but also employees and executives.

Man in the middle attack (MITM): fraudsters intercept data between your site and users. It's the digital equivalent of eavesdropping on a conversation, using techniques such as SSL stripping or Evil Twin attacks, that mirror WiFi access points to capture data.



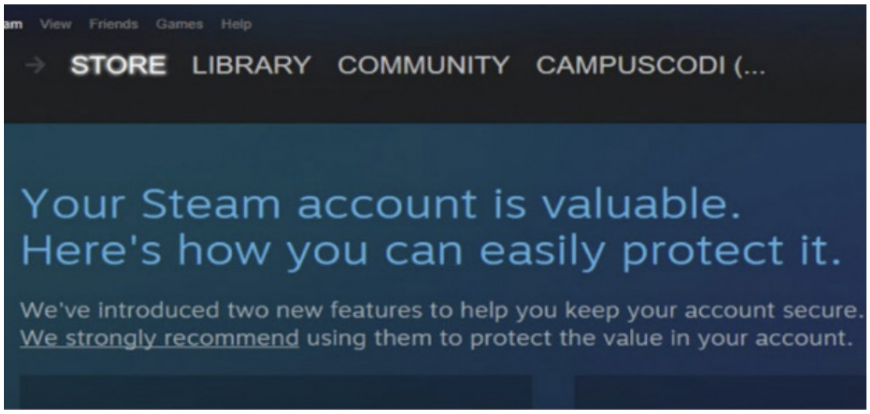
SIM-Swapping: remember some of the high-profile names at the beginning of this guide? Most of their accounts were stolen via SIM-swapping or SIM-jacking attacks. It's when fraudsters contact telecom operators to take control of a mobile phone number. Because so many accounts are verified via 2FA (2 Factor Authentication), gaining access to a number means you can log into someone's Instagram, Twitter, etc.

XSS to ATO: XSS stands for Cross-Site Scripting. It allows criminals to execute scripts in a victim's browser, often with the goal of setting up new passwords on preexisting accounts.

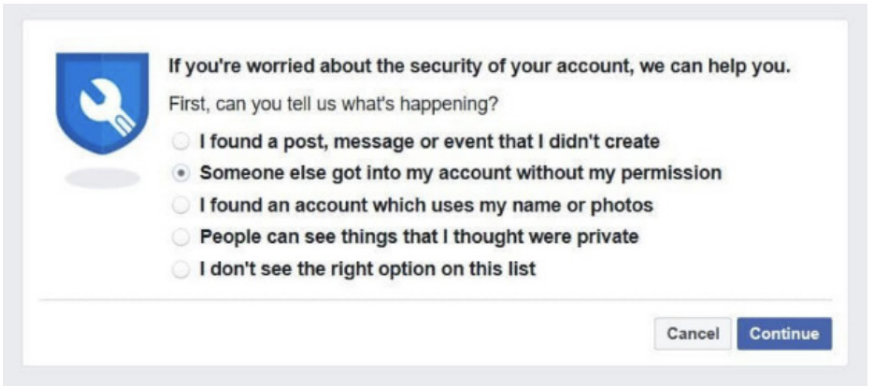
You can read a more in-depth post about account takeover scenarios here.

Part 2: Protecting Accounts

Before focusing on blocking account takeovers, it's worth delving into the steps you can take today to improve your protection.



How games marketplace Steam encourages 2FA use



Facebook's ATO reporting feature

8 Ways to Protect Yourself from Account Takeovers

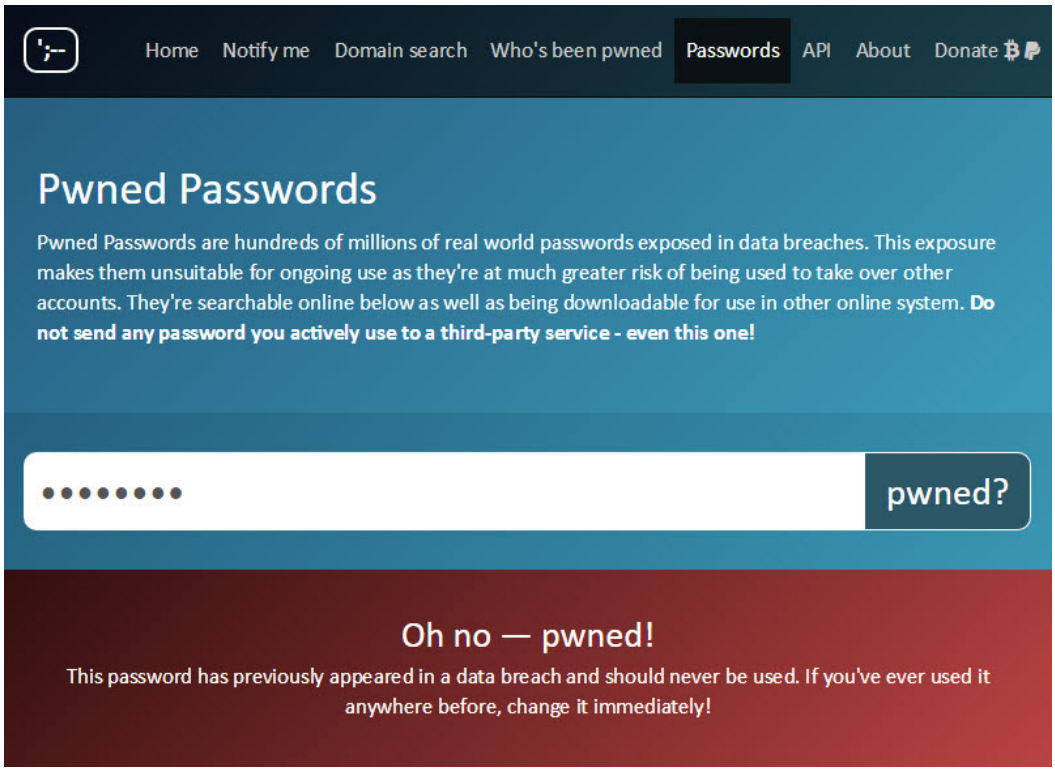
Letting your users and employees understand how valuable their accounts are is a great way to make life harder for fraudsters.

Common sense applies, but you should also make a coordinated effort to remind people to:

- **Stop reusing passwords:** losing one account can have few bad consequences. Losing all your online accounts can be disastrous.
- **Update passwords regularly:** you could even check if your data has been leaked in a breach (via the Have I Been Pwned website for email addresses) and ensure your password is quickly updated after major ones.
- **Use password managers:** they will generate strong passwords, store them and autofill as needed.
- **Be vigilant with links:** especially from unknown email senders, poorly written text, or suspicious web pages. It's always better to access important sites manually when possible, i.e.: by typing the URL directly into your browser.
- **Double-check URLs:** watch out for signs of a phishing attempt if the URL or web page looks unusual (for instance: www.paypall.com).
- **Enable MFA (multi-factor authentication):** two-step verification (2SV) or two-factor authentication (2FA) are easier to use than ever thanks to third-party apps like Google Authenticator.
- **Use a VPN:** especially when connected to public WiFi networks

Then you should also be open about the risks of ATO, and communicate regularly with users about changes affecting their accounts.

This could be an email to let them know a new phone number has been registered or to confirm their recent conversation with a customer representative.



Check to see if your password(s) have been exposed.

6 Ways to Improve Your Security for Account Takeovers

From the company side, it's best to follow the best data protection practices: this is for data that is collected, transferred, processed, and accessed.

- **Use SSL:** especially on pages that collect sensitive information such as credit cards, social security numbers, or addresses.
- **Encrypt whenever possible:** not just for logins, but also for communications.
- **Secure physical devices:** particularly important for company phones, laptops and desktop computers – especially in a work-from-home setup.
- **Hire 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.

> **Double-check user passwords:** You can use Troy Hunt's Pwned Passwords2 (or K-Anonymity if you're a Cloudflare customer) to check if a user's credentials have been leaked before. This is useful to warn them on registration if they are about to use a leaked password, or to trigger an email verification on logins to make sure they are not a victim of an ATO."

- Restrict HTML input, sanitise values and use Allowlist values to ensure your site code is clean.

Consider User Friction

In an ideal world, you'd be able to set up as many authentication and verification steps as you need to ensure users are who they say they are.

In practice, these steps are serious obstacles in your customer journey. Adding more friction, whether at signup or login, is the surest way to send users towards more lenient competitors – especially in today's always-on economy.

So how do you balance security and friction? **By deploying invisible authentication tools.**

Part 3: How to Deploy Authentication Tools for Account Takeovers

In many ways, authentication tools have the same goals as the ones you use for onboarding or KYC. It should be about giving you 100% confidence you're allowing the right user on your site.

The good news is that the best fraud prevention tools will work for monitoring, investigating and blocking ATO attempts. Here's what you should deploy today:

Real-Time Data Enrichment

A key challenge of detecting suspicious logins is that data is often limited. In fraud prevention, the more data points you have, the more accurate your decision can be. At that touchpoint, we usually have an IP address, device information, and basic customer behaviour.

Still a single data point can be enough to blacklist login attempts, provided that data is enriched in real-time to confirm its validity.

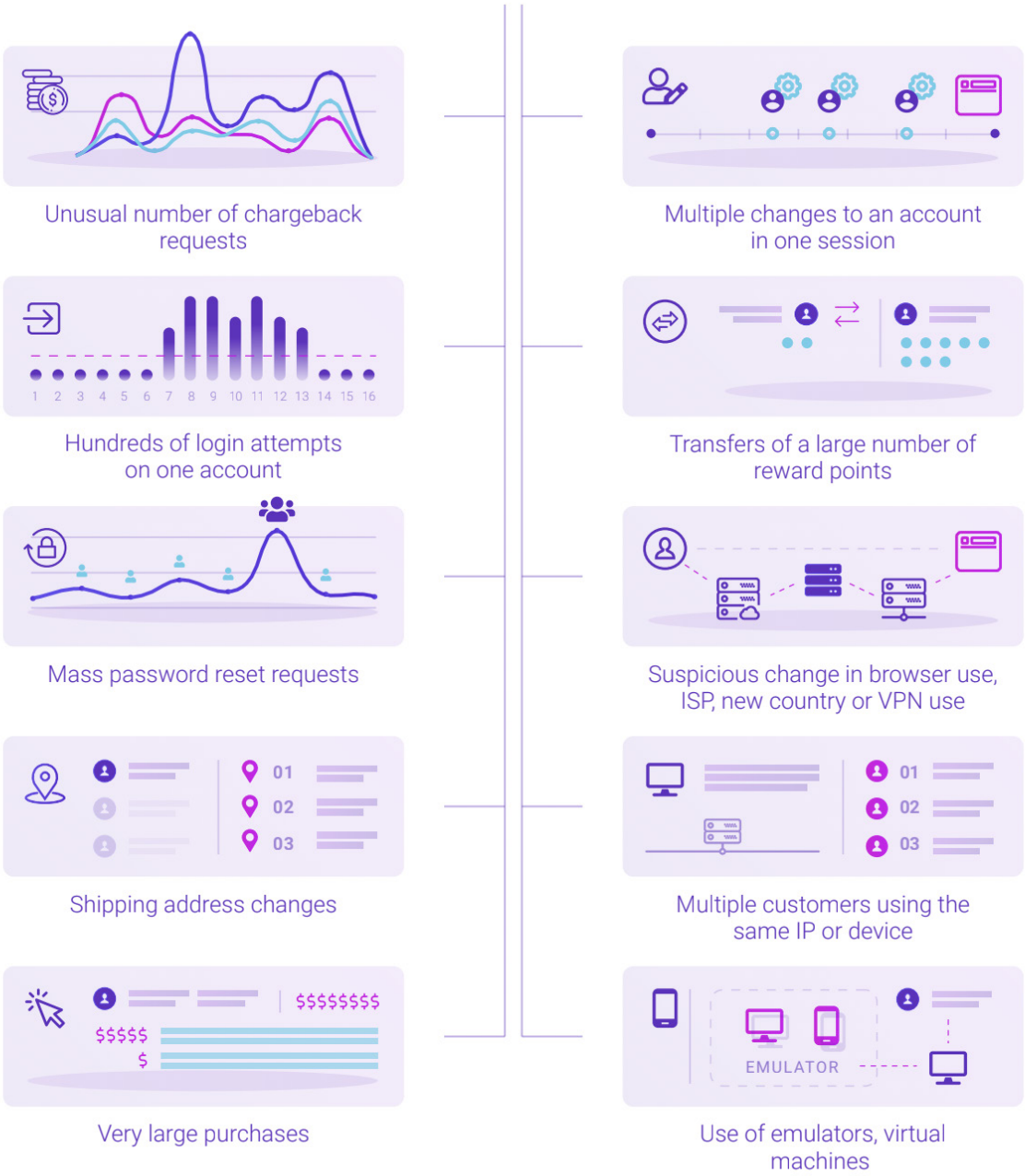
Device fingerprinting: by creating a device hash/ID using data from a browser, operating system, device and network, you can flag suspicious connections. This is something that doesn't require excessive calculations, yet can be highly effective in preventing the users from logging in with unknown devices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

IP Analysis: the classic fraud prevention method that can be enriched to reveal suspicious VPNs proxies or TOR usage.

Logging that data can also be useful to create whitelists for your users to reduce false positives. For instance, a user could let you know they're travelling in advance, which should be reflected in their IP address whitelist.

You can learn more about device and browser fingerprinting in our guide here.

Behaviour Analysis Through Velocity Rules



If an ATO is already underway, your only chance is to spot suspicious user behaviour. Whether it's inspected through a dedicated fraud prevention system or manually, here are the signs an ATO attack might have happened.

The key here is to have rules in place that let you understand what is considered safe behaviour and what should raise flags.

Dynamic Friction

In spite of your efforts to deploy invisible security layers, there will still be cases when grey areas may confuse the system.

That's when you shouldn't be afraid to bring out the big guns with heavier authentication methods. These include:

- **Selfie ID**
- **Voice message**
- **2FA**

But as we've previously mentioned, these high-friction tools should be a last resort only. It's much easier to offer a smooth authentication experience if your anti-fraud tools allow you to control the thresholds of what's acceptable and what demands more investigation.

At SEON, for instance, we allow fraud managers to adjust the thresholds of their risk scores, so that they may allow or reject logins based on the company's risk strategy.

How SEON Does ATO Protection

At SEON, we've built in a number of ATO prevention features in our end-to-end fraud detection platform. We took great care to put user experience front and centre, reducing the processing time to a minimum while allowing you to leverage:

- **Powerful device fingerprinting:** to instantly know when a user is connecting with a suspicious combination of software and hardware.
- **Whitebox machine learning:** SEON's algorithm learns from your ATO patterns and retrains itself numerous times a day. You get results via human-readable rules, which you can use to backtest your login data to test false positives rates.
- **Velocity rules:** Collect and screen complete user activity on your website via custom API calls related to any data point you want. It's the closest thing to behaviour analysis to help you understand when someone is acting suspiciously.
- And much more...

The good news is that protecting an account and your general business interests can be done with the same tools. As long as you have all the flexibility and customization options of SEON risk rules and API calls for fraud protection.

SEON

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900