sift

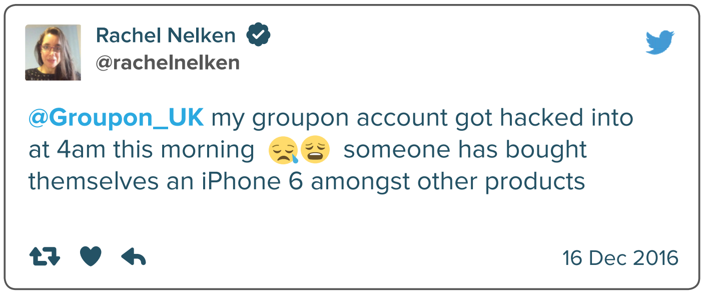
Complete Guide to Preventing Account Takeover

Contents

Introduction

In December 2016, a Groupon user named Rachel casually checked her email and was shocked by what she found. A message in her inbox confirmed her successful order for an iPhone 6, bought using her Groupon account. But Rachel never made that order. Someone else had gained access to her account without her permission.

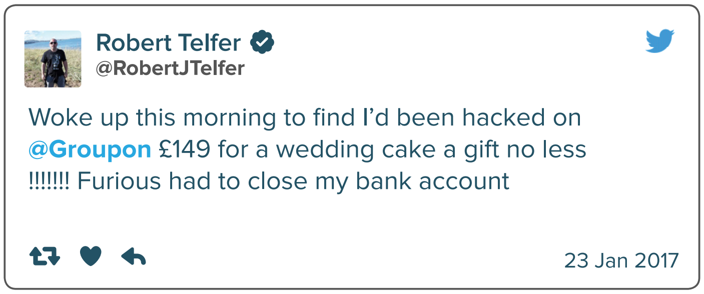
She—and a handful of other victims of account takeover (ATO) at the coupon site—soon took to social media to voice their frustration about the situation.



Rachel Nelken
@rachelnelken

@Groupon_UK my groupon account got hacked into at 4am this morning 😞😩 someone has bought themselves an iPhone 6 amongst other products

16 Dec 2016

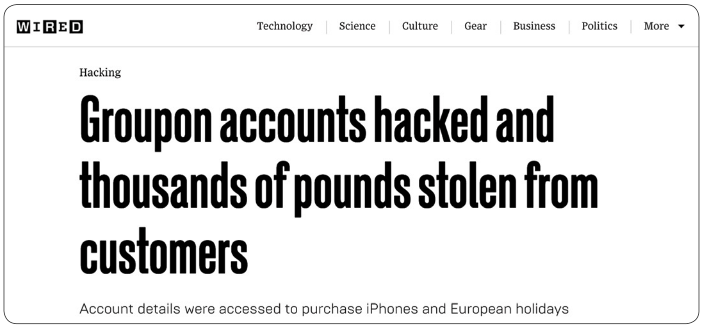


Robert Telfer
@RobertJTelfer

Woke up this morning to find I'd been hacked on @Groupon £149 for a wedding cake a gift no less !!!!!!! Furious had to close my bank account

23 Jan 2017

And major news publications picked up the story, too:

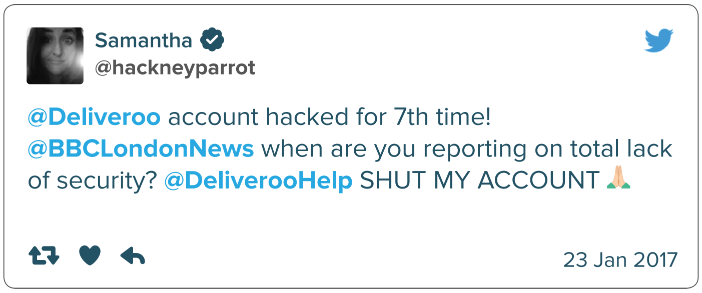

WIRED
Technology | Science | Culture | Gear | Business | Politics | More

Hacking

Groupon accounts hacked and thousands of pounds stolen from customers

Account details were accessed to purchase iPhones and European holidays

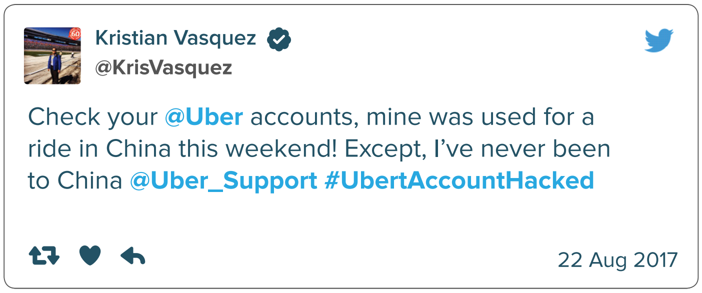
Groupon is hardly the only brand—or the largest—to see their name in the headlines due to an ATO attack. Organizations ranging from Deliveroo to the UK National Lottery have suffered high-profile ATO attacks.



Samantha
@hackneyparrot

@Deliveroo account hacked for 7th time! @BBCLondonNews when are you reporting on total lack of security? @DeliverooHelp SHUT MY ACCOUNT 🙏🏼

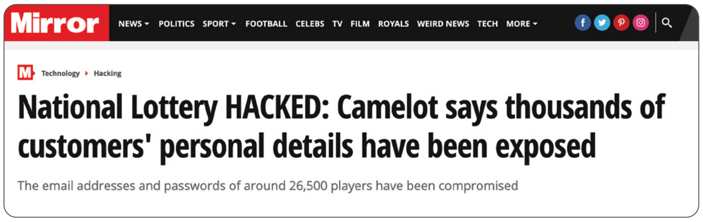
23 Jan 2017



Kristian Vasquez
@KrisVasquez

Check your @Uber accounts, mine was used for a ride in China this weekend! Except, I've never been to China @Uber_Support #UbertAccountHacked

22 Aug 2017


Mirror
NEWS POLITICS SPORT FOOTBALL CELEBS TV FILM ROYALS WEIRD NEWS TECH MORE
Technology › Hacking

National Lottery HACKED: Camelot says thousands of customers' personal details have been exposed

The email addresses and passwords of around 26,500 players have been compromised

Some of the most well-known ATO cases involve celebrities and major social networks. Remember when Mark Zuckerberg had his Twitter, Pinterest, and LinkedIn accounts hacked (and the organization behind it claimed it was because the Facebook CEO was using insecure passwords that were easy to crack)? Or when Katy Perry had her Twitter account compromised? Or the NFL? The list goes on and on.

The brand damage done by ATO is palpable, immediate, and very visible to consumers. But before we go any further, let's cover some basics... what exactly is ATO?

Online businesses' latest foe: compromised accounts

ATO, also known as account compromise, is just what it sounds like: a bad actor getting access to a good user's account. Once that access is achieved, the fraudster can use the account for all kinds of opportunistic and malicious ends. As part of the ATO, the fraudster may change the user's password to lock them out, and change their email address so the good user doesn't receive any additional communication about activity on their account.

How fraudsters profit from ATO

- using up stored credits or rewards points
- making high-value purchases
- buying digital goods
- scamming other users, phishing
- creating fake listings
- spamming
- selling the credentials on the black market
- extorting money from the legitimate account owner
- assuming the identity of the real user

Any website or app where users have accounts is at risk of ATO. Criminals may target e-commerce sites, banks, gaming sites, marketplaces, social networking sites—any site where they can extract value from an account. The challenge for these businesses is to quickly and accurately detect fraudulent logins—protecting their users and their brand reputation—without getting in the way of their good users.

Like so many other types of fraud, ATO is increasingly committed at scale by bots, as well as manually. Hackers write scripts that test various combinations of stolen usernames plus potential passwords across multiple websites and apps, until they find a way in. These brute force attacks are helping fraudsters move as quickly as possible and focus on maximizing the value of each successful ATO. Researchers at Shape Security found that criminals can have as much as a 2% success rate by using these automated attacks.

ATO IN ACTION

What does ATO look like? Here's an example from a ticketing site:

Fraudster accesses account through hacked credentials bought on the dark web

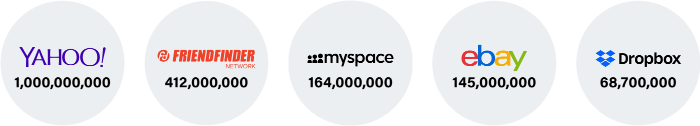
Changes the password so real account holder can't access

Adds a stolen credit card to the account and uses it to buy tickets

Creates listings to sell the tickets they just bought fraudulently

More data breaches = more ATO

How did ATO gain such traction over the past few years? You need only look at the big cybersecurity headlines to get a clue. We've entered the era of the data breach.



Source: Information is Beautiful

The scale and sophistication of breaches is growing. 2016 brought us a revelation of the first billion-account breach at Yahoo. Some of the year's other notorious breaches—and revelations of breaches—included social sites (LinkedIn, Dropbox, AdultFriendFinder), the government (U.S. Department of Justice, Internal Revenue Service), and universities (UC Berkeley, University of Central Florida). Some 554 million records were compromised in the first half of 2016 alone, according to the Gemalto Breach Index.

The downstream effect of more data breaches? A rise in ATO. Perhaps unsurprisingly, ATO is one of the fastest-growing forms of fraud and abuse.

All of those credentials floating around on the black market lead to a rise in the number of individual sites like Groupon suffering ATO attacks. It's becoming clear that a password—no matter how complex—is no longer sufficient to protect a user's account.

48%

of online businesses observed a rise in ATO last year

$2.3b

losses from ATO in 2016

61%

increase from the year before

Source: Sift Digital Trust & Safety Survey, 2019

How fraudsters get ahold of credentials

Data breaches are one fruitful source of personal information. Here are some other ways that criminals get their hands on users' login credentials.

Phishing with fake websites

Have you ever received an email from a service you trust, but something seems a bit off—like the "from" field or a URL? A Gmail phishing scheme in early 2017 brought renewed attention to a form of cyberattack where criminals set up a website to look exactly like it belongs to a company someone's familiar with—down to the fine print at the bottom of the page. Then, they email potential victims to try to get them to click on the link. Without carefully checking the site address, someone could easily give over their login details.

Malware, Trojans, spyware

Another danger of clicking on unknown links is malware. For example, following a malicious link can inadvertently download key-loggers that track what people are typing into login and password fields. A keylogger called iSpy was recently tracked by security researchers, who discovered it could access passwords stored in web browsers, record Skype chats, take screen shots with a webcam, and steal software licenses.

Social engineering

In February 2016, The U.S. Department of Justice fell victim to a hacker posing as a new employee who was struggling to log in to the department's online portal. He was given a temporary token that gave him full access to data including email addresses and credit card numbers.

Social engineering attacks like these use psychological tools to manipulate users into giving up confidential data. Criminals may call customer support and convince someone to give them access to a user's account (especially if they know some personal info, like SS#). Or they may send a phishing email to a company, carefully designed to look like it came from an executive at that business, asking someone to turn over sensitive information.

Hijacking a mobile device

The U.S. Federal Trade Commission reports an uptick in mobile phone hijacking, where a criminal gains access to a user's mobile account. A thief can make use of a ton of sensitive information if they have access to a mobile phone, including payment credentials. And sophisticated fraudsters can also make use of a victim's phone number to get two-factor authentication text messages that allow them to access bank accounts and other sensitive information.

Mining social media

Have you listed your hometown or high school on a public social media profile? If so, know that fraudsters who easily discover this information may use it to crack passwords on sites that use "standard" security questions. Other common personally identifiable information that people list on social media include birth dates, children's names and birthdays, addresses, and phone numbers.

Why ATO is attractive to fraudsters

It's no secret that people are moving more and more of their lives online. Increasingly, the internet is where people meet, date, engage on social issues, read news, and so much more. Websites and apps don't just have access to one data point—for example, a credit card—they hold an entire digital identity.

Meanwhile, the fraud prevention community could be seen as a victim of its own success. As the industry gets better at detecting some types of fraud, criminals move on to an alternative method. For example, there's already been ample evidence that EMV has been pushing fraud from physical credit cards to the online channel. But increased security measures like EMV may also be leading more criminals to try their hands at ATO. More online businesses are also beefing up their payment fraud detection capabilities, which further squeezes fraudsters' revenue sources and causes them to look for alternative ways to make money.

As fraudsters look to monetize different forms of data, the price of non-payment-related account information has been driven higher and higher on the black market. Researchers in 2016 found that account credentials command more money on the dark web than payment information

How much credentials are worth on the black market

Uber	NETFLIX	facebook	Credit card bundles
$3.78	$0.76	$3.02	$2.22

Source: TrendMicro

Let’s delve into a few more reasons why fraudsters are flocking to account data:

Built-in trust

New accounts are more likely to be flagged for fraud or given more scrutiny. Because the account already exists and is connected to a legitimate user, the fraudster is effectively camouflaged and more difficult to detect.

Richer data

Stolen identities or accounts are a richer form of data than credit card numbers—they can even be used to create new accounts.

Longer shelf life

Login credentials can typically be used for longer than credit card numbers. A consumer can easily cancel their card with a phone call, but it’s much harder to “cancel” all the accounts where they use their email address.

Businesses playing catchup

We already mentioned that the technology used to prevent fake accounts and credit card fraud is becoming more widely employed and more sophisticated. However, many websites are not yet set up to detect ATO. Fraudsters can do a lot of damage before they’re discovered.

New opportunities

Modern business models are introducing new ways for criminals to monetize the information they steal—like setting up fake Uber driver accounts and charging “phantom” rides to stolen accounts. Account ransoms using Bitcoin are also on the rise.

Lax password practices

Despite numerous warnings to not reuse passwords on multiple sites and apps, studies show that more than half of people do just that. Since so many people use the same username and password on multiple sites, one batch of compromised info could potentially unlock accounts all across the web.

SURVEY SHOWS

59%

of people reuse passwords on multiple sites

ONLY

8%

of people use a password manager product

Source: Password Boss

Damage done by ATO

The damage done by ATO occurs on multiple fronts: negative PR, legal and compliance implications, a drop in the value of your customers, financial loss, and more. One of the more easily identifiable costs of ATO attacks is chargebacks. If a thief is using a legitimate user's stored credit card information—or adding a compromised card number to a real user's account—you're on the hook for lost goods and chargeback fees.

As we saw earlier, being associated with ATO can also be disastrous to your company's brand. Why? Accounts can feel very personal to users. Knowing that a fraudster had control of their account—and access to their personal information—can feel intrusive, and may raise concerns about your company's security protocols. Unlike some other forms of fraud, ATO places the victim smack in the middle of disputes, which can cause confusion, doubt, and anger.

As an example of how an individual could be affected by a single ATO, imagine if you had your Facebook account taken over, but you didn't immediately realize it. Your friends might contact you, asking you why you're suddenly selling Ray-Ban sunglasses or posting obscene images. Maybe someone clicks on a rogue link that "you" posted, and their computer gets infected with a virus. Maybe the hacker deletes some of your photos, or changes your personal information. Who knows what private info they've been digging around in? It's like someone broke into your house, messed everything up, and now you have to clean it up.

ATO may also be more difficult and costly for a consumer to resolve than other types of fraud. Think about it: if a consumer's credit card number is stolen and used fraudulently, not only is the crime typically detected quickly by the issuer or merchant's fraud detection system, but if the victim does discover a rogue transaction on their credit card statement they have zero liability for any purchases made.

With ATO, on the other hand, a consumer is more likely to discover fraudulent activity themselves. The victim may also encounter more customer support gray areas and delays when sorting out the problem. That's because many online businesses are playing catchup when it comes to both detecting and handling ATO. It's a new form of online criminal behavior that is growing rapidly and requires a new mindset to thwart.

ATO VICTIMS PAY OUT OF POCKET

A single user pays an average of **$263 out of pocket** to resolve ATO.

Collectively, victims spent **20.7 million hours** to resolve ATO in 2016.

Source: Javelin Strategy & Research

Measuring the impact of ATO

Outside of counting your company lucky for not being in the headlines, how do you measure whether ATO is a problem for your business? ATO can be harder to quantify than payment fraud. There aren't always chargebacks involved. And as we mentioned earlier, losing customers' trust and suffering brand damage are some of the most common—and serious—effects of ATO.

However, it is possible to put a price on lost user engagement with your site or app. We'll walk you through a way to do this, based on calculating the lifetime value (LTV) of a user:

Collect active inputs

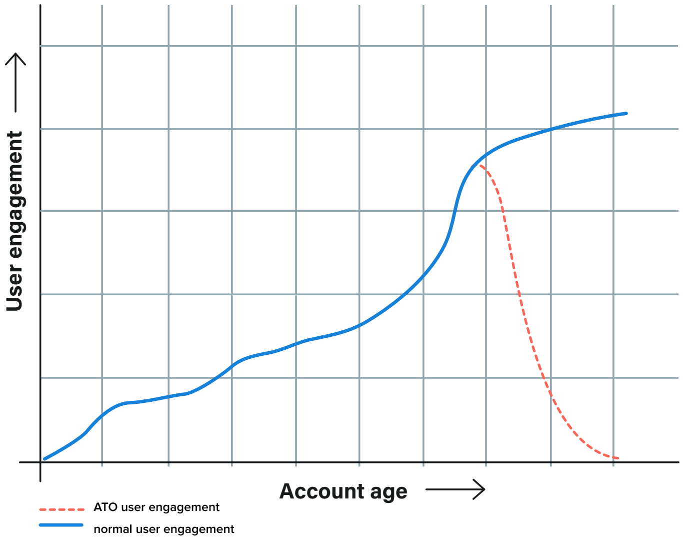
This bucket encompasses every complaint and reported ATO. You can find this information by asking Customer Support how many tickets, inbound phone calls, chats, and emails they've received that mention ATO. If you aren't formally tracking this information, it's a good idea to start now.

Collect passive inputs

But not every ATO victim proactively reports what happens to them. Some simply stop using a website or service, while others close their account altogether. One way to gauge passive ATO damage is to analyze all of the users who have deactivated their account. Do a post-mortem on a sample or each one (depending on volume), trying to determine whether they have suffered ATO.

Measure how ATO affects engagement

Once you have gathered both active and passive inputs, you can compare the LTV of an affected user to that of a normal user. For an e-commerce site, this value may be measured in terms of money spent. For a social site, it could be how often they visited or engaged on the platform.



Compare the delta between the ATO affected user and the normal user. That will give you a sense of how ATO is affecting your business from a monetary perspective.

Detecting and preventing ATO

ATO prevention is becoming a priority for more online businesses who want to protect themselves and their valuable users. That brings us to the nitty-gritty: how do you tell the difference between a login from legitimate user and a fraudster?

Behavioral clues

Many of the signs of ATO are contained in subtle behavioral patterns across all of a user's activity. An effective ATO prevention tool is able to synthesize a range of activity and identify the anomalies. Here are some of the separate signals that may point to a potential ATO:

- Login attempts from different devices and locations
- Switching to older browsers and operating systems
- Buying more than usual, buying higher priced items
- Changing settings
- Changing shipping addresses (especially just before ordering)
- Changing passwords
- Multiple failed login attempts
- Unusual log out attempts. (It's unusual for users to log out of certain services.)
- Suspicious device configurations, like proxy or VPN setups

But not every ATO victim proactively reports what happens to them. Some simply stop using a website or service, while others close their account altogether. One way to gauge passive ATO damage is to analyze all of the users who have deactivated their account. Do a post-mortem on a sample or each one (depending on volume), trying to determine whether they have suffered ATO.

Implementing smart ATO prevention

When seeking to protect users' accounts, many online businesses may introduce security checks like 2-factor authentication, email links, SMS codes, captchas, and even phone calls. When used selectively and intelligently, these checks can be a powerful tactic to prevent ATO. However, when used over-aggressively, they can be extremely disruptive to the user experience. The key, as with any type of fraud prevention, is to get as close as possible to the ideal balance that minimizes risk from bad users while also minimizing friction for good users. But how do you achieve that balance?

Dynamically adjusting the login experience

If you're using a tool that can provide a risk score, you can dynamically adjust the login experience for risky users. For example, if a user's score is low, then you can remove all friction so they can easily sign in and keep engaging on your platform without being bothered with captchas or codes. On the other hand, if the score is high, you have the option of adding authentication steps to ensure that the user is really who they say they are. You could, for example:

- Email or text the user a one-time passcode to enter after login to confirm their identity.
- Email or text an account link that the user can click to approve the new login from a new device.
- Email or text the user a notification of a login from a new device so that they can be aware in case it's not them.
- Limit a user's account actions (e.g., no updating password, no placing orders) until the user logs in again from a trusted device or location.
- Have user fill out a Captcha or image identification.

You could choose to use a combination of the methods above to provide different levels of friction, based on the amount of risk. When applied appropriately intelligently, these authentication steps not only minimize your risk, but could even increase users' trust in your site's security, and by extension their trust in your product or service. You've got their back.

Sift Account Takeover Prevention

Sift Account Takeover Prevention was designed to help businesses achieve a perfect balance of strong fraud defenses and an excellent user experience. ATO Prevention uses machine learning and advanced behavioral analysis to keep bad actors from accessing legitimate users' accounts, while guaranteeing as little interruption to the login process as possible.

How Sift ATO Prevention works

With a simple integration, we'll be able to ingest and analyze your users' behavior, and then compare that behavior with patterns of good and bad behavior on your site and across our network. Then, each time someone logs in, we'll return an ATO risk score in real time—so you can instantly identify risky users and dynamically alter their login experience.

To calculate a score, our technology looks at a range of potential ATO signals, such as:

- user browsing patterns
- network and IP data
- location history
- device information

We also leverage years of data we've already collected across our vast customer network of more than 6,000 sites and apps.

Fewer account takeovers
Stop illegitimate account access and malicious activity on trusted user accounts.

Better user experience
Reduce login friction for valid users, making account access simple yet secure.

Chargeback prevention
Prevent fraudulent transactions and incurred chargeback fees by stopping account hacking before it begins.

Conclusion

In this new world of ongoing data breaches, sophisticated phishing attacks, and personal information changing hands on the dark web, all online businesses must come to terms with their vulnerability to ATO.

No company wants to be the next brand making headlines for the wrong reasons, with users publicly complaining that their accounts were hacked, their personal information compromised, their lives inconvenienced. However, with the proper tools and guidance you can not only protect your business, but also enhance the the overall user experience. You can not only avoid brand damage, but build long-term brand loyalty.