# Account Takeover

Account takeover (ATO) should be familiar to anyone who uses the internet and online accounts. You may have received an email from Gmail or Twitter while you were on vacation or traveling for business that tells you a suspicious login occurred. It’s because the geographic location the application is familiar with has changed and the automatic API sends you a warning. Basically they want to ensure that it’s you. However these warnings should not be taken lightly. ATO is one of the fastest growing and most persistent threats for consumers on the internet today.

ATO is an attack in which a hacker gets into your account by stealing your login credentials. Once there they are for all intents and purposes you. These attacks are undertaken with the usual ploys like phishing, social engineering, [credential stuffing](https://www.hcaptcha.com/credential-stuffing-what-it-is-and-how-to-stop-the-attacks), and malware. Administrators are prized targets because they’re the guardians of a plethora of user accounts in a system.

### ATO Fraud

ATO often leads to ATO fraud, which can take many forms, beginning with something as innocuous as an online purchase and going all the way to the depletion of bank accounts. Sometimes ATO is just a recreational activity like vandalism, but more often than not it’s the result of professional hackers looking to make a score. The bigger the score the better, so professionals focus on high value targets. Even so it’s a horrific violation on any scale. Imagine finding a thousand dollars on your credit card and struggling to remember when you made the purchase, then slowly coming to the realization that you’ve been the victim of ATO.

ATO fraud is only growing. It has more than doubled since 2020. Part of the reason for this is the proliferation of online purchasing due to the pandemic, in which many more people were staying at home, and another peculiar reason is the rise of the online loyalty program, in which online vendors try to retain their loyal customer base with programs similar to air miles. These loyalty programs are a form of currency for hackers. Many companies have learned the hard way that this has to be taken much more seriously.

The bulk of security has been invested in the checkout process. Unfortunately for the digital consumer, the number of vulnerabilities has expanded far beyond the checkout, and the personal vulnerability is almost limitless once a hacker gains access to even one of your online accounts. One of the problems is the number of online accounts people have today.

Most internet users will have at least one hundred online accounts and typically only use a dozen of them regularly. The other eighty or ninety are completely forgotten. Here’s the thing hackers exploit — most people will use the same username and password over and over again.  
Despite countless prompts and even suggestions for complex passwords, most people will stick to their old habits, familiar names, birthdays, and other habits.

### Preventing ATO Fraud

There are any number of ways an account takeover can happen, but they most boil down to a handful of techniques. Probably the best known is phishing. This is when you get fooled into turning over login credentials.  
Another technique is what security insiders call social engineering. Somebody might impersonate a trusted source and ask that login credentials be revealed. Malware like key loggers are often used as well. There’s a technique called [credential stuffing](https://www.hcaptcha.com/credential-stuffing-what-it-is-and-how-to-stop-the-attacks), which is a little bit like what they call *ground and pound* in mixed martial arts. This is where previously compiled lists of stolen credentials are stuffed into multiple attempts to breach online accounts. The final technique is the one for which the user must take the most responsibility, weak passwords.

The best way to [avoid Account Takeover](https://hcaptcha.com/enterprise) is to use long and complex passwords for each account. Get out of the habit of repeating the same password and username over multiple accounts. Most operating systems come with password managers now to generate and store complex passwords. There’s no excuse.

If the service provider has enabled multi-factor authentication then use it. This adds an extra layer of security. Most ATOs are through a single point of access. If there’s a backup to the security like a text message sent to a phone they won’t be able to get into your account.

Never give personal information to an unknown email messenger. This is one of the main ways hackers gain access to your accounts. The scams are nearly limitless. This has even worked on people by hackers pretending to be the revenue service of their country, informing them that their taxes have been reassessed and that they owe more money, and further inciting them by stating that if the money is not paid within a fixed period of time, usually a very short window, penalties and interest on penalties will apply.

Always keep your software, your applications, and your operating system up to date. Download and install all recommended patches and security updates. ATO professionals are experts at exploiting short windows of time between new security patches and old systems. Never for a moment think that your adversary is undisciplined or lazy. Professionals are as patient and disciplined as any jungle predator. Getting into your online accounts is how they eat.

Maintain a good knowledge of all your accounts. Remember little details. Keep a close watch on things and make sure nothing changes. If you notice anything strange investigate it right away. Always address correspondence from the legitimate application software owners. They’re there to help you. They have a working familiarity with your use of the tool and generally from where you use it. Any anomalies in this usage will be documented in an email. Make sure that if you do get an email from the software proprietor that it’s authentic. Always be wary of a message that asks you to log in right away and change your password.

Invest in security. Stay informed about the latest technology and methodologies for thwarting ATOs. This is true for everybody but especially important for system administrators who are the gatekeepers for large reservoirs of data and online account information. Invest in fraud detection and systems to respond to anomalous behavior. There have been significant advances in artificial intelligence (AI) and machine learning (ML). Real-time monitoring for behavior anomalies is becoming an essential market requirement for reputational integrity. The best defense is awareness of the problem. Stay informed and stay security minded.