BEYOND IDENTITY

How Beyond Identity Protects Against Account Takeover Attacks

Account takeover (ATO) is no joke. This tactic involves a malicious actor gaining access to an account through compromised credentials. The attacker uses the account for illicit activities, from stealing intellectual property to conducting fraudulent transactions.

Adversaries use multiple tactics, including purchasing and reusing leaked usernames and passwords, credential stuffing, or social engineering to gain access to these credentials. Regardless of the tactic, the number and cost of account takeover attacks are increasing.

The COVID-19 pandemic has only made things worse. Sift Security found that account takeover attacks increased three-fold from 2019 to 2021, while Javelin noted a 90% increase in 2021 alone.

The costs of account takeover recovery are even more alarming and are hard to quantify as they involve both consumer and business ATO incidents. However, experts have estimated the total costs to be around $12 billion in 2021, three times what it was three years earlier.

The old way of stopping account takeover attacks

The traditional method of stopping account takeover attacks has long been implementing password-based multi-factor authentication (MFA). Initially implemented by financial firms to stem an increasing tide of online account hacks, MFA is now the most commonly used method across all industries to add an additional level of security to the traditional username and password.

MFA has undoubtedly made it much more difficult for cybercriminals to use compromised credentials. However, it was only a matter of time before attackers figured out ways to hack traditional MFA.

How does this happen? Traditional MFA still relies on a password as one of the factors, which are easily compromised. Other MFA factors often aren't that secure

either: one-time passwords, notifications, magic links, and texted or emailed codes are all phishable factors.

This is especially problematic for public-facing industries. Those organizations usually hold a significant amount of sensitive information about their customers, who expect it to be well protected. Here are some industries that face challenges with account takeover attacks:

- **Financial technology (fintech):** Fintech companies have much to lose if attackers break in so they must keep their customer's data and money safe while adhering to strict compliance standards. Certainty of identity is vital. Traditional MFA does not provide that, and the increasing number of high-profile hacks in the news is evidence the industry isn't prepared.
- **E-commerce:** These companies store highly personal financial data on their customers. Identity theft incidents can come about because of data breaches on e-commerce websites, and these breaches are costly to organizations. It's not unusual for companies to spend millions in mitigation efforts when dealing with breaches.
- **Travel:** Travel company customers are on the move, making location-based authentication difficult. They often access applications from insecure access points, like public Wi-Fi networks. To prevent breaches, it's important to ensure the person is who they say they are with strong authentication.
- **Media:** While paywalls add substantial friction to the authentication process, the costs of producing quality web content are not cheap, so paywalls have become a necessary evil. But that hasn't stopped tech-savvy subscribers from trying to find ways around these security measures, and password sharing is common, which can lead to breaches and security incidents.

Organizations across these organizations and elsewhere have turned to MFA to gain back the upper hand against cybercriminals. But with MFA failing, it's time for a newer and more modern authentication method.

How Beyond Identity stops account takeovers

As long as the password remains, the risk of account takeover remains, regardless of whether or not an organization deploys MFA. Beyond Identity uses technology that eliminates the password once and for all.

The bottom line?

Moving to passwordless authentication eliminates all password-based attacks.

Through Beyond Identity's passwordless authentication platform, which includes Secure Customers, you can eliminate the password and dramatically improve security through modern, phishing-resistant MFA.

Passwordless authentication stops account takeover attacks because it eliminates the password and the security issues around stolen, leaked, and reused login credentials are gone. Attackers can't breach password-protected sites or steal passwords to log in because Beyond Identity's unphishable cryptographic credentials are the key—not passwords. Your customers can rest easy knowing their information is behind multiple unphishable factors.

Passwordless solutions that employ multiple secure factors are ideal, and our platform only uses unphishable factors, like biometrics, cryptographic security keys stored in the Trusted Platform Module (TPM) of the device, and device-level security checks. You can also set up risk signals that work for you, including location, recent activity, device security posture, and more, to enforce real-time security. They can vary based on the user, device, and sensitivity of the data accessed, and are checked continuously throughout the user session. The result? Continuous protection against account takeover attacks.

Your users will love no longer having to create or constantly rotate passwords, and they won't have to deal with lockouts. Beyond Identity makes the login experience a breeze—with no second device or temporary code required.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.