SpyCloud

6 Myths About Account Takeover (ATO) Prevention Strategies

Think you're doing enough?

Account Takeover (ATO) is real and it's growing at an alarming rate. The world runs on passwords, people reuse passwords, and criminals are still relying on that fact to perpetrate ATO.

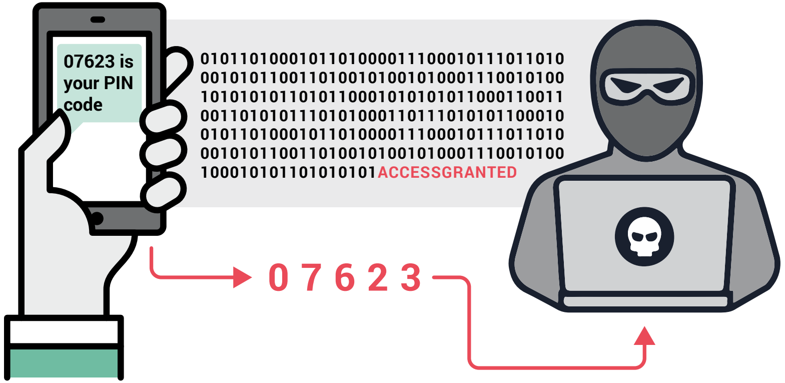
- ⚠ The **#1** most common breach action over the last 4 years (2017-2020) has been the use of stolen credentials.
- ⚠ On average, people over 55 only use **12 passwords**, while Millennials use **8** and Gen Z uses just **5**.
- ⚠ **59%** of people use the same password everywhere, and the average person has **200** online accounts that require password identification.
- ⚠ Only **45%** said they'd change their password following a data breach.
- ⚠ **43%** of logins submitted through most sites are account takeover attempts.
- ⚠ The cost of ATO to U.S. businesses alone exceeds **$5B**. What is ATO costing your business?

Think standard security measures provide 100% protection from account takeover?

Think again. We analyzed 6 of the most popular "ATO prevention strategies" and what we found was more myth than fact.

Myth 1: **Multi-Factor Authentication**

- ⚠ In most countries, **less than 33%** of businesses are using MFA: 28% in the US and Canada, 29% in Australia, and 33% in the UK.
- ⚠ **<10%** of Gmail users have 2FA enabled.



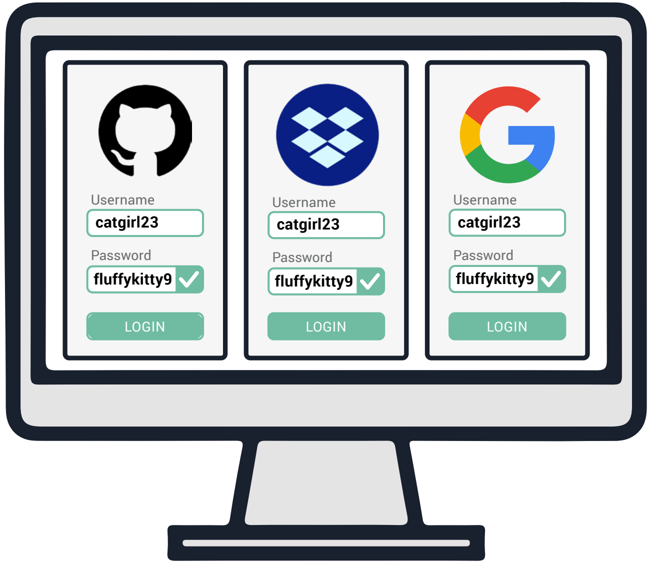
MFA doesn’t stop all ATOs because:

- ⊗ Adoption remains low, despite continued education.
- ⊗ Personally identifiable information (PII) is often exposed on social media, and criminals use it to guess account security questions.
- ⊗ Password reuse exposes multiple accounts.
- ⊗ Criminals use phishing and SIM-swapping to intercept codes.

See p. 11 for sources

Myth 2: **Password Managers**

- ⚠ Only **23%** of internet users use password managers.
- ⚠ In organizations that don't require password managers, **53%** rely on human memory to remember their passwords.
- ⚠ **30%** are using high risk strategies such as writing their passwords down in a notebook.



Username
catgirl23
Password
fluffykitty9 ✓

Username
catgirl23
Password
fluffykitty9 ✓

Username
catgirl23
Password
fluffykitty9 ✓

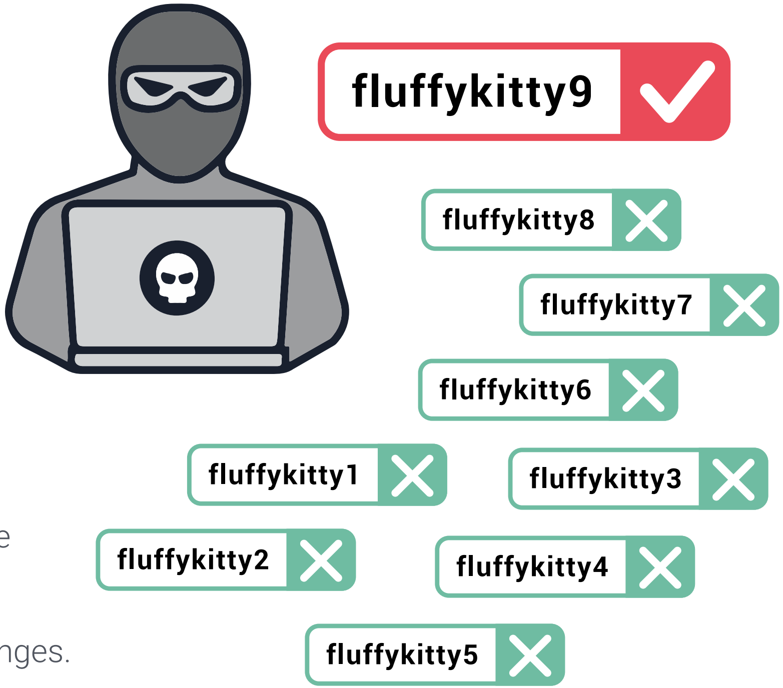
Password managers haven't stopped ATO because:

- ⊗ Most employees don't use password managers at home.
- ⊗ Employees log into work accounts on personal devices.
- ⊗ More than **76%** of people reuse the same password across multiple accounts.
- ⊗ Criminals will try a breached password on multiple accounts.

See p. 11 for sources

Myth 3: **90-Day Password Rotations**

- ⚠ Password reuse enables the next password to be guessed in **< 5** guesses.
- ⚠ **41%** of passwords can be guessed within 3 seconds.
- ⚠ **60%** of passwords can be cracked with automated tools.



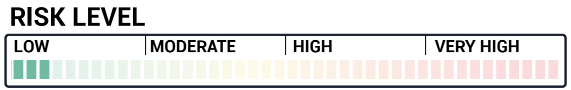
90-day password rotations aren’t effective in preventing ATO because:

- ⊗ Users most often begin with a weak password.
- ⊗ Users often change their passwords in predictable, guessable ways (e.g. fluffykitty8 to fluffykitty9).
- ⊗ Attackers use malware to enable access after password changes.

See p. 11 for sources

Myth 4: **Behavior or Heuristic-Based Solutions**

- More than **350,000** new malware programs are reported daily.
- Phishing attacks have increased **250%** year over year.
- In 2019, organizations reported experiencing a median of **922,331** credential stuffing attempts.



Behavior or heuristics-based solutions don’t always work because:

- Threat actors have adapted to countermeasures.
- They have an operational impact on applications which can negatively impact the customer experience.
- Sophisticated criminals are less likely to tip off artificial intelligence.

Myth 5: **Deep & Dark Web Scanners, Crawlers and Scrapers**

- ⚠ **>90%** of the information on the internet is in the deep web and is not accessible by surface web crawlers
- ⚠ The average time to identify and contain a breach is **280** days.
- ⚠ Fullz, or the full stolen information on a victim, can be sold on the dark web for just **$30-$40**.

Scanners, crawlers and scrapers miss valuable intel because:

- ⊗ Stolen credentials are rarely posted in their entirety on dark web forums.
- ⊗ Scanners only pick up redacted samples, not the fullz.
- ⊗ Fullz can only be obtained through covert relationships with threat actors.
- ⊗ Automated tools are incapable of finding fullz that humans can.

See p. 11 for sources

Myth 6: **Corporate Policy**

⚠ **76%** of companies lack a policy about using personal email on corporate networks.

⚠ **7%** have a policy against personal apps on corporate networks but don't monitor.

⚠ **50%** of users use the same passwords for their personal and work accounts.

Corporate policies aren't enough to prevent ATO because:

⊗ 20% of workers don't follow company security policies all the time.

⊗ Threat actors target corporate accounts using reused personal account passwords.

⊗ Criminals send malware to employees who follow corporate policies, or find other ways to exploit them.

⊗ Cybercrime tactics evolve faster than corporate policies can be established.

See p. 11 for sources

Choose the **Right Solution**

When evaluating ATO prevention solutions, ask hard questions:

- ✓ Can this solution detect a potential compromise early, before criminals have the chance to do harm?
- ✓ Can this solution automate remediation of accounts vulnerable to compromise?
- ✓ Does this solution include access to plaintext exposed credentials?

Cybercriminals are smart.

Your ATO prevention solution needs to be smarter.

SpyCloud

For the best ATO prevention possible, backed by the industry’s highest quality, most actionable breach database

SpyCloud is the leader in ATO prevention, protecting billions of employee and consumer accounts globally. The vast majority of the compromised data we collect from third-party breaches comes from human intelligence (HUMINT), enabling us to find exposed credentials early in the ATO lifecycle – before automated tools know they exist on the dark web.

With our automated password remediation, we enable busy security teams to scale.

Learn more & check your ATO exposure at spycloud.com

Sources

Think you're doing enough?
1. Verizon Data Breach Investigations Reports 2017-2020; https://spycloud.com/a-deep-dive-into-the-verizon-2020-data-breach-investigations-report/
2. https://www.ibm.com/security/data-breach/identity-report-user-study
3. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/logmein-lastpass-survey-ebook-v8.pdf
4. https://www.zdnet.com/article/google-launches-password-checkup-feature-will-add-it-to-chrome-later-this-year/
5. https://securityintelligence.com/why-you-should-drop-everything-and-enable-two-factor-authentication-immediately/
6. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

Myth 1:
1. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LMI0828a-IAM-LastPass-State-of-the-Password-Report.pdf
2. https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google

Myth 2:
1. https://www.helpnetsecurity.com/2020/05/18/use-password-manager/
2. https://www.techrepublic.com/article/57-of-it-workers-who-get-phished-dont-change-their-password-behaviors/
3. https://www.helpnetsecurity.com/2020/05/18/use-password-manager/
4. https://spycloud.com/spycloud-research-breach-exposure-of-the-fortune-1000/

Myth 3:
1. https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Myth 4:
1. https://www.av-test.org/en/statistics/malware/
2. https://www.cpomagazine.com/cyber-security/phishing-attacks-now-more-common-than-malware/
3. https://spycloud.com/a-deep-dive-into-the-verizon-2020-data-breach-investigations-report/

Myth 5:
1. https://www.experian.com/blogs/ask-experian/wp-content/uploads/dark-web-infographic.jpg
2. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
3. https://www.darkreading.com/vulnerabilities---threats/complete-personal-fraud-kits-sell-for-less-than-$40-on-dark-web/d/d-id/1335362

Myth 6:
1-2: https://www.computereconomics.com/article.cfm?id=1060
3. https://www.lastpass.com/state-of-the-password/global-password-security-report-2018
4. https://www.securitymagazine.com/articles/92992-of-workers-dont-follow-company-security-policies-all-the-time