6 Myths about ATO Prevention Strategies

Don't Believe the Hype

Account Takeover (ATO) is real and it's growing at an alarming rate:

- ⚠ The **#1** most common breach action in 2017 was the use of stolen credentials[1]
- ⚠ On average, people over 55 only have **12 passwords,** Millennials have **8** and Gen Z only have **5. 59%** of people use the same password everywhere.[2]
- ⚠ **43%** of logins submitted through most sites are account takeover attempts.[4]

Think your ATO prevention efforts provide 100% protection because a vendor said so?

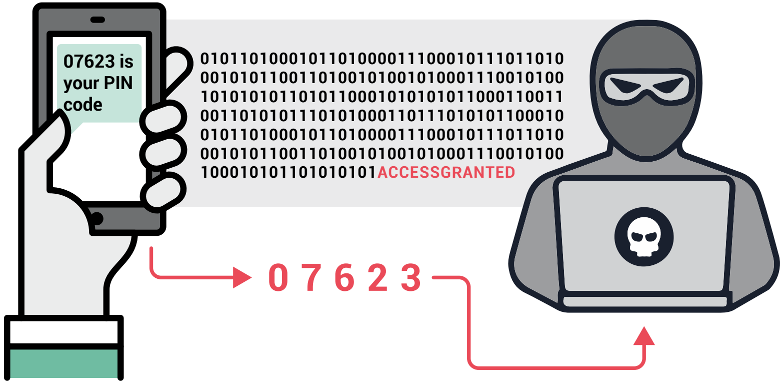
Think again. **We analyzed six of the most popular ATO prevention strategies and what we found was more myth than fact**

Myth 1: **Multi-Factor Authentication**

- ⊗ 2FA use has decreased or **barely increased** from 2010 to 2017[5]
- ⊗ **>10%** of Gmail users have 2FA enabled[6]
- ⊗ **>10%** of Gmail users who used 2FA had issues inputting a code delivered by SMS[6]

2FA hasn't made much of a dent in ATO prevention because:

- ⊗ Few people know about it or use it
- ⊗ Personally identifiable information (PII) is often exposed on social media
- ⊗ Criminals use PII to guess account security questions
- ⊗ Password reuse exposes multiple accounts
- ⊗ Criminals use phishing tools to steal access codes

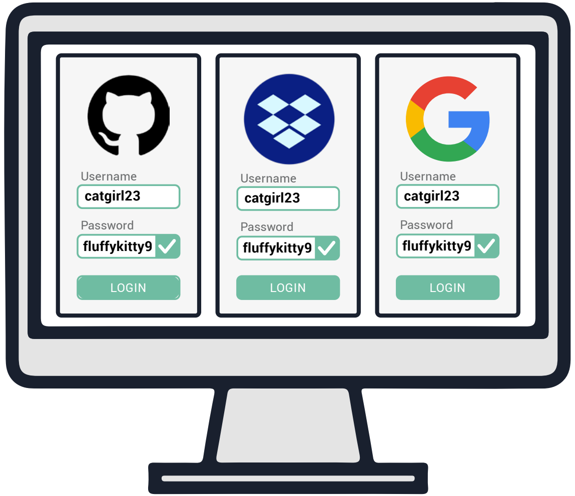


Myth 2: **Password Managers**

- **12%** of internet users use password managers[7]
- **3%** of internet users say using password management software is the password technique they rely on most[7]
- **30%** of adults worry about the overall security of their online passwords[7]

Password Managers haven't stopped ATO because:

- Most employees don't use password managers at home
- Employees log into work accounts on personal devices
- **87%** of people reuse the same password across multiple accounts[8]
- Criminals will try a breached password on multiple accounts



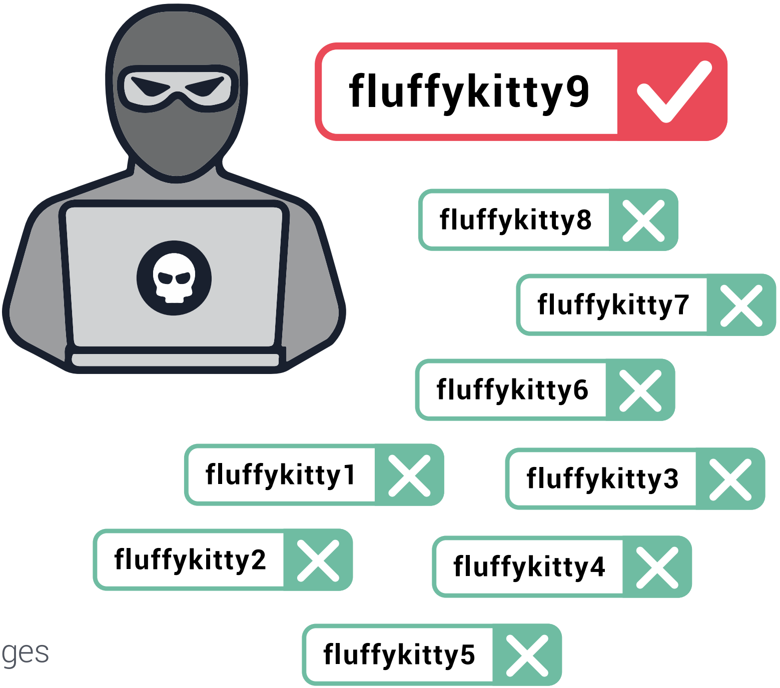
Username
catgirl23
Password
fluffykitty9 ✓

Username
catgirl23
Password
fluffykitty9 ✓

Username
catgirl23
Password
fluffykitty9 ✓

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

- Password reuse enables the next password to be guessed in **< 5** guesses[9]
- **41%** of passwords can be guessed within 3 seconds[9]
- **60%** of passwords can be cracked with automated tools[9]

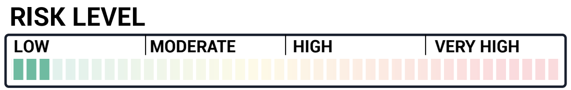


90-Day Password Rotations aren't effective in preventing ATO because:

- 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

Myth 4:
Behavior or Heuristic-Based Solutions

- More than **390,000** new malware programs are reported daily[10]
- The third most common breach action in 2017 was phishing attacks[1]
- Phishing attempts have increased by **65%** in 2017[11]
- The click rate of phishing emails after opening a previous phishing email is **20%**[1]



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 Artifical 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[11]
- ⊗ 3B compromised Yahoo accounts weren't disclosed for **2 years**[12]
- ⊗ Fullz, or the full stolen information on a victim, can be sold on the dark web for around **$100 per record**[13]

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

Myth 6: **Corporate Policy**

- ⊗ **76%** of companies lack a policy about using personal email on corporate networks[14]
- ⊗ **7%** have a policy against personal apps on corporate networks but don't monitor[14]
- ⊗ **46%** of employees admitted to transferring files between work and personal computers[15]

Corporate Policies aren't enough to prevent ATO because:

- ⊗ Threat actors target corporate accounts using reused personal account passwords
- ⊗ Criminals send malware to employees who follow corporate policies
- ⊗ Cyber crime tactics evolve faster than corporate policies can be established
- ⊗ The majority of employees admit to not following corporate policies[16]

Choose the **Right Solution**

No solution on the market is 100% effective at preventing ATO. Any vendor who claims otherwise should be suspect. All of these ATO prevention solutions miss critical elements in fortifying your defenses against ATO.

When evaluating products and capabilities:

- ✓ Ask hard questions
- ✓ Determine which vendors are selling hype and which can back up their claims with data
- ✓ Watch a live demo in your own environment

The cyber criminals are smart. They adapt.
Your security solution should do the same.

SpyCloud

For The Best ATO Prevention Possible

SpyCloud is a leader in ATO prevention, monitoring and recovery. We use automated technologies, of course, but rely on human intelligence (HUMINT) to find compromised credentials early in the ATO lifecycle - before automated tools know they exist on the dark web.

We go a step further by providing actionable mitigation capabilities, such as forced password resets when stolen credentials are found.

To find more information visit spycloud.com

Sources

1 2018 Verizon Data Breach Report

2 https://www.lastpass.com/psychology-of-passwords (registration required)

4 https://securityintelligence.com/why-you-should-drop-everything-and-enable-two-factor-authentication-immediately/

5 https://www.statista.com/statistics/789942/us-use-of-two-factor-authentication/

6 https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/

7 http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/

8 https://mashable.com/2017/02/28/passwords-reuse-study-keeper-security/#dQk2ht4jU8qT

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

10 https://blog.barkly.com/how-to-stop-cyber-attacks-behavior-based-protection

11 https://blog.dashlane.com/phishing-statistics/

12 https://www.experian.com/blogs/ask-experian/wp-content/uploads/dark-web-infographic.jpg

13 http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

14 https://venturebeat.com/2015/02/08/fullz-dumps-and-cvvs-heres-what-hackers-are-selling-on-the-black-market/

15 https://www.computereconomics.com/article.cfm?id=1060

16 https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

17 https://www.csoonline.com/article/2123363/compliance/3-reasons-why-employees-don-t-follow-security-rules.html