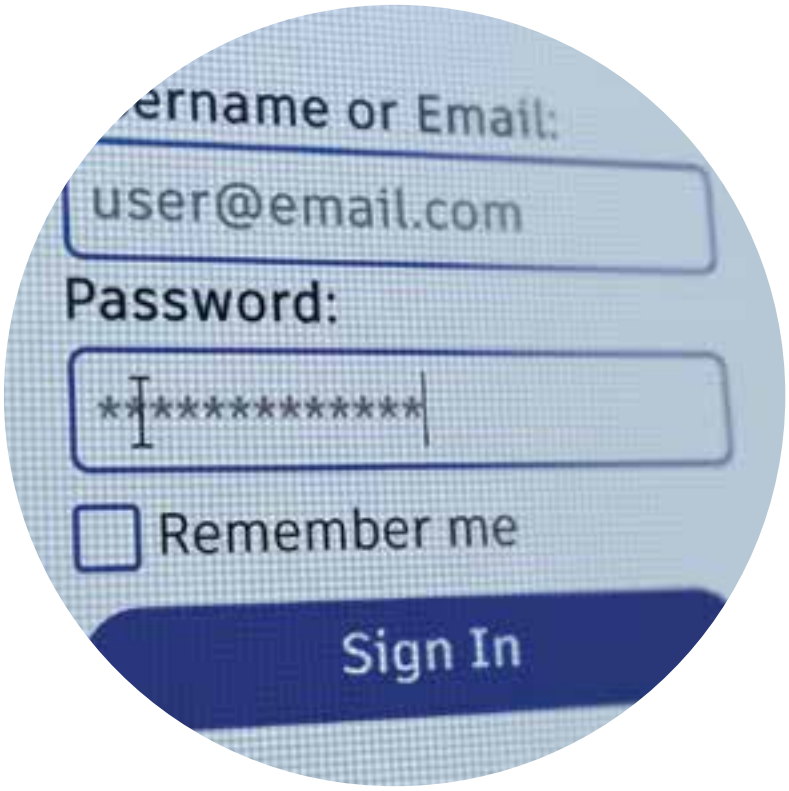
WHITE PAPER

Credential and Password Reuse

By: David Montague
and Justin McDonald



Too many consumers use the same credentials across multiple sites, apps, and logins—even after being notified of a breach that exposed those credentials. Nevertheless, consumers blame a site or app for account takeover due to their use of compromised credentials, not themselves. To mitigate brand risk, it's incumbent on organizations to prevent the reuse of compromised credentials by their customers and users.

>50%

More than half of people in the US say they reuse the same password across more than one online account

PASSWORD HYGIENE

A system is only as secure as its most vulnerable point of exposure, and the weakest link in the chain of cybersecurity is us: the user. It is a natural tendency to default to the path of least resistance, to remember a few passwords instead of fifty. Consumers have a propensity to use the same username or email address in tandem with the same password across a multitude of sites, apps and logins. Many are guilty of reusing at least one password more than once.

According to a Google and Harris Poll[1], 52% of US consumers reuse the same password across two or more accounts, while 13% admit to using the same password across ALL accounts. This is corroborated in the myNetWatchman case study of "Company M" as well.

Consumers will change their passwords after being notified that a password has been compromised in a data breach, right? This type of notification is a feature that some web browsers support when a known-to-be-compromised password is entered, or consumers may be notified directly by the organization who suffered the breach, confirming compromise of their password or other personally identifiable information (PII). Sadly, no, even this doesn't seem to invoke the impetus to replace a compromised password on other sites.

Another Google and Harris Poll[2] found that just 45% of Americans would update their password after knowing it was compromised in a data breach. For about two-thirds of them, this would require updating that password across multiple accounts, so fewer than half of US consumers take the time to do so.

Data breaches are so frequent and seemingly ubiquitous in terms of how many of us they impact, consumers may be suffering from data breach fatigue. Knowing your password was compromised is different than the imminent threat of knowing attempts to use your compromised password are actively on-going, with the latter likely to inspire significantly more urgency on the part of the consumer. Or more likely, if an organization has these insights about a specific user and password, they can require this password be changed.

CREDENTIAL STUFFING AS A GATEWAY ATTACK

Now consider the compounding effects of the volume of breached credentials exacerbated by the attitudes of impacted consumers, sometimes bordering on apathetic. Companies are at risk due to the magnitude of compromised passwords available to bad actors, the inherently insecure tendencies of most consumers, and the ability of these bad actors to use technology such as botnets to test stolen credentials en masse, i.e., credential stuffing attacks.

Compromised credentials are a gateway to more sensitive and more valuable consumer data and Personally Identifiable Information (PII). A nefarious user with a compromised password may be after more PII or account access to use directly, or they will build a more complete stolen identity profile to sell at a higher price. Credential stuffing attacks leverage the already-stolen password and take advantage of the fact that around two-thirds of consumers reuse passwords, using botnets to find websites where the compromised password is shared and still in use.

> "Based on the billions of account compromise events we have seen, customers do reuse passwords across websites and most won't change their password even if it is breached on another website. We have even seen credentials work that we know were breached years ago."
>
> David Montague, CEO
> myNetWatchman

Credential stuffing is to account takeover what card testing is to third party fraud. Just as a bad actor will test compromised payment card numbers to see which are active then use those cards to make fraudulent purchases, a bad actor will use a botnet to test a trove of username and password combinations across many sites to see where the same pair of credentials are also used.

Data breaches, even those from years ago, provide consumer credentials that are not only still in use, but still in use across multiple logins or accounts. Credential stuffing attacks are the means to maximize the value of those stolen credentials, at the expense of the consumers and the organizations with whom those consumers conduct business or hold their accounts. The security flaws enabling data breaches at one organization have a ripple effect that impacts many more organizations down the line. Consumers' lackadaisical and insecure password practices then put the onus of security on the organizations where they hold their accounts.

Less than half of consumers would update their password after learning that it was compromised in a data breach

IT'S UP TO ORGANIZATIONS TO SECURE ACCOUNTS

We applaud the consumers who never use a password more than once and change them with any inclination that they may have been compromised. Unfortunately, that is the exception not the rule. As a result, organizations need a strategy to identify users that should either be presented a form of additional, or step-up, authentication or be forced to complete the password reset process. Like fraud prevention at the transaction event, this must strike a balance between risk mitigation and user experience, relying on risk signals to determine when more friction is warranted.

One way to identify these at-risk accounts is to check user credentials against lists of username and password combinations that have been compromised together in external data breaches.

Even this, however, is likely to cast too big of a net, and forcing all users who reuse these compromised credentials will impact many who may never be targeted at your site.

A more nuanced approach is to identify the accounts that are actively being targeted with ATO attempts. Not just knowing that a customer or employee is compromised, but that those compromised credentials are actively being attempted at other sites, which justifies the friction of step-up authentication or requiring a password reset.

Most companies collect limited data and therefore have a limited perspective on risk activity occurring at the login event, but seeing failed login activity, password tumbling and other activity before a successful login are valuable signals that should be considered when making decisions at subsequent event stages like a transaction or account profile changes.

> "Retail eCommerce web-sites are often the target of credential stuffing and account takeover attacks, yet most companies do not connect login activity, login failures, or testing to the financial transactions or account changes that occur next."
>
> Rob Long, CTO
> myNetWatchman

Two Factor Authentication (2FA)

Two Factor Authentication (2FA) is a great tool for step-up authentication, but it should not be applied universally to all users and all logins for most organizations other than some industries where this is expected, such as with financial institutions. Collecting more actionable signals at the login event enables organizations to be much more strategic and selective about when 2FA is presented or when to force a password reset.

Many consumers who reuse credentials compromised in a data breach and later fall victim to ATO on an account with another organization will blame that company for that ATO rather than take any personal responsibility.

It is in each organization's best interest to protect against the brand risk associated with ATO, even when resulting from reused passwords. This means being aware of accounts at a higher risk of ATO, cultivating the risk signals to gain this visibility into a user

account's ATO risk level, and leveraging that data as a means to present 2FA or require a password change when it is warranted. myNetWatchman provides the data and visibility to enable this.

Credential stuffing is the path of least resistance for ATO attacks, and simply put, ATO events are damaging and expensive. It's hard to put a monetary value on the brand damage, but one place to start is the lost lifetime value of customers who no longer engage with or transact with an organization where their account was compromised.

According to a survey from Sift[3], 74% of consumers would stop using a site or app if their account was compromised. The direct financial loss to organizations related to ATO varies widely based on their industry, as this tends to be most damaging for financial institutions and financial services. According to Security.org[4], the average financial loss for ATO victims is $12,000, which will often be reimbursed by the organization. Juniper Research[5] estimates the direct financial cost per ATO event to be $290, a figure likely to be in-line with what merchants and organizations outside of the financial sector will experience.

> The case study of myNetWatchman client "Company M" showed that 10% of the credentials successful at Company M had been successful (valid) at other sites prior to being tested at Company M

52%	CONSUMERS WHO REUSE AT LEAST ONE PASSWORD [1]
13%	CONSUMERS WHO USE THE SAME PASSWORD FOR ALL ACCOUNTS [1]
22.6%	SHARE OF LOGINS THAT ARE ATO ATTEMPTS [6]
91%	CREDENTIALS TESTED ON OTHER SITES BEFORE USED IN ATTACK
$290	AVERAGE COST OF ATO PER ACCOUNT [5]

Compiling the various statistics related to password reuse and ATO, it is apparent that credential stuffing attacks are lucrative for fraudsters as they can monetize or add value to stolen credentials

which are relatively easy to use and reuse against a multitude of organizations online. Keep in mind that these statistics are related to ATO of consumer accounts but the cost of ATO against workplace accounts held by employees or contractors is significantly higher. ATO targeting workplace users can lead to data breaches, customer data or proprietary data being held ransom, rerouting of payable or receivable accounts and other schemes that could bankrupt an organization.

DETECT CREDENTIAL STUFFING ATTACKS

Many organizations won't realize they are being targeted with credential stuffing attacks. Here are some common signs to look for:

1. **Risk exposure to credential stuffing –** Consider the value of user accounts to a bad actor. Having stored value or stored payment instruments that can be used to transact within user accounts, or being able to access services once logged in.

2. **High volume of failed login attempts** – Failed login attempts are rising or have been high for some time. Failed logins occur in spurts of activity across many different accounts/usernames. There are many failed login attempts that are not just an incorrect password, but attempting a username that is not registered or does not exist.

3. **Persistent ATO problems** – User complaints or notifications of ATO are common or on the rise. There is a notable spike in users changing their passwords. Note that many dormant accounts may fall victim to ATO and the real user will not know or follow up. For every known ATO event there can be many more that remain undetected.

Early detection of credential stuffing is key, as it enables organizations to resolve and prevent issues before they grow to be more costly and more disruptive to the user base. An organization

> "Breaches occur every day, in the first quarter of 2024 alone there were 734 data breaches announced from companies with over 28.4 million customers potentially impacted.[7] When these events happen, they will lead to credential stuffing attacks on sites like yours to see if these consumers or employees were reusing the same credentials on other sites. Here at myNetWatchman we see 15 million credential stuffing events a day by bad actors. It pays to know it is happening."
>
> David Montague, CEO
> myNetWatchman

with high ATO risk exposure needs to catch this activity before the account is used to transfer funds or spend stored value. Merchants can spend less time and resources screening transactions from accounts that have been taken over if those nefarious users never make it to the stage where they are able to transact.

It's one thing to detect credential stuffing based on apparent bot activity, but the sophistication of bots to mask or change IPs presents challenges. It's better to have insights on when compromised credentials are being attempted, and that's where access to proprietary myNetWatchman data provides value.

Most organizations are limited to the data they see at their own site, but myNetWatchman aggregates data across the internet to see credential stuffing as it unfolds. Data on passwords and usernames used in tandem and known to be compromised in breaches is leveraged to protect organizations when those same compromised credentials are used on their sites. Further, not just knowing that the credential pair has been compromised, but that it has recently been used or attempted elsewhere online, is a strong and high-quality risk signal. myNetWatchman is actively looking at live activity across bad actors to detect when millions of compromised credentials are actually being used.

At that point, whether it's a nefarious user or the real one, there is reason to force a password reset. Depending on the value or sensitivity of information protected by the user account's login credentials, the user could be presented with the requirement to change their password the next time they attempt to log-in, or they could be prompted to change their password via email before they attempt a login on their own. The messaging should be clear that the organization forcing the change did not suffer the data breach, but the password is a shared credential between the company forcing the password change and the one who suffered the data breach.

> Bad actors can buy not only compromised credentials on the dark web, but also the bots or bot kits to carry out credential stuffing attacks

There are multiple stages when password screening and forced resets should occur. A best practice is to screen passwords users input at the new account creation stage. Messaging can be clear, that the password is not acceptable because it is known to have been compromised in external data breaches while associated with the same username or email provided. Any time a new password is chosen, whether at account creation or later if an existing account chooses to update the password on their own accord, this new password should be screened.

CONCLUSION

Data breaches and stolen passwords are prevalent while consumers have a propensity to reuse them. Bad actors exploit this with credential stuffing attacks, growing the impact of a data breach beyond the organization who suffered the breach directly to disrupt consumers and their accounts across a multitude of other sites, apps and logins.

Part of managing user accounts is managing this ATO risk exposure and fighting back against credential stuffing attacks to protect your user base, their user experience, as well as the services, monetary funds and PII protected within their user accounts.

Detecting credential stuffing attacks as they occur, as well as detecting the attempted use of compromised passwords, enables organizations to mitigate ATO risk and stop a potential attack before it grows more disruptive and more costly. One level of increased protection is to consider the fact that a username and password combination has been compromised in a data breach at any time in the past. While this is a signal of elevated risk, it is a broad signal that doesn't necessarily mean the current login attempt is ATO. The next level is a more nuanced approach that looks at not just data breach data, but data across the web on credential stuffing attacks to see that a pair of credentials is not just compromised but actively being used in credential stuffing attacks.

When a new user account is created or an existing user changes their password, wouldn't you like to know if they are reusing credentials that have been compromised elsewhere?

myNetWatchman's data enables organizations to make dynamic, risk-based decisions on each user or login attempt

This is valuable insight that influences when to present two factor authentication or force a password reset, and more importantly, when NOT to require these measures.

ABOUT myNETWATCHMAN

myNetWatchman has been providing cyber fraud intelligence data for more than 20 years to retailers, financial services, insurance, and other industries. With over 10 years of live data surveillance, the company has protected over 800 million users and has in our data repository over 35 billion exposed credential pairs—with 15+ million newly-exploited logins added each and every day.

myNetWatchman continuously captures live fraudster use of over 15 million credentials a day on the dark web and from live collection sources and has amassed more than 35 billion compromised credential pairs

myNetWatchman

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech

1 - https://services.google.com/fh/files/blogs/google_security_infographic.pdf
2 - https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf
3 - https://pages.sift.com/rs/526-PCC-974/images/Sift_Account-Security-Guide_eBook-062823.pdf
4 - https://www.security.org/digital-safety/account-takeover-prevention/
5 - https://miracl.com/blog/account-takeover-fraud-to-exceed-25-billion-in-2020/
6 - https://internetretailing.net/40-of-traffic-to-ecommerce-sites-comes-from-bots-raising-cyber-security-threat-level/
7 - https://www.idtheftcenter.org/publication/itrc-q1-data-breach-analysis/