Passwords IN THE Enterprise

STATE OF PASSWORD USE REPORT 2020

Balbix®

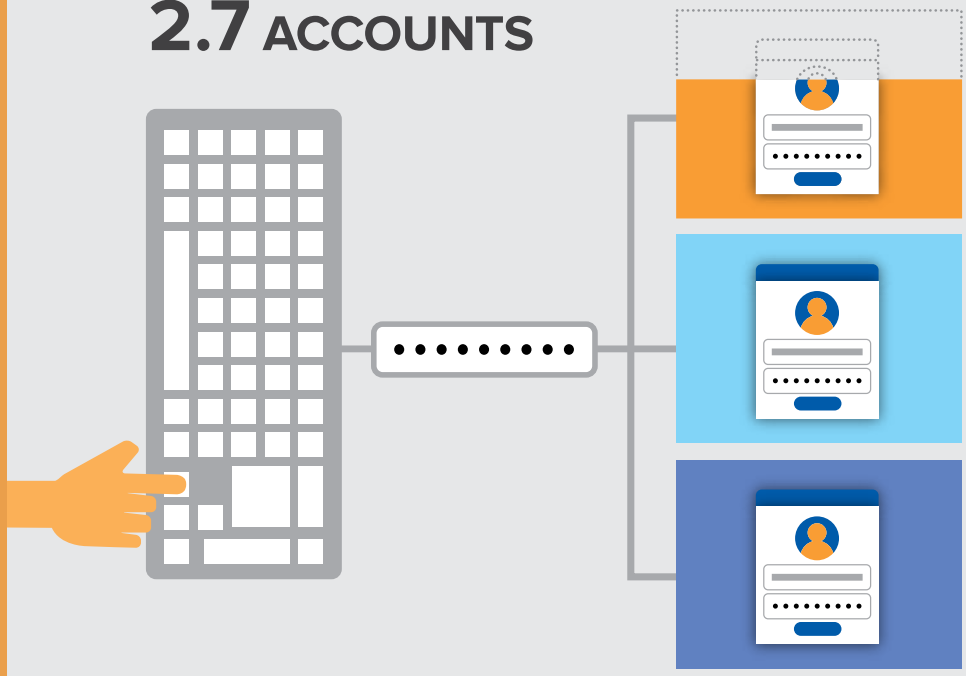
Despite years of warnings and monumental efforts across the industry to get enterprises and consumers to improve their password hygiene, compromised credentials still account for a whopping 80% of hacking-related breaches due to compromised, weak and reused passwords.

In early 2020, the Balbix Security Analytics Team set out to determine whether this is the result of a small minority of users with poor credential protection, or a much more widespread issue. The findings clearly show that despite the warnings, very few take appropriate action to significantly reduce the risk of password compromise.

KEY FINDINGS

MORE THAN
99%
OF USERS
REUSE PASSWORDS, EITHER ACROSS WORK ACCOUNTS, OR BETWEEN WORK AND PERSONAL ACCOUNTS

ON AVERAGE, EVERY SINGLE PASSWORD IS SHARED ACROSS
2.7 ACCOUNTS

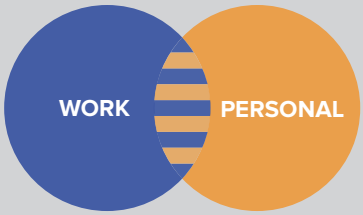


Balbix®

The average user has more than

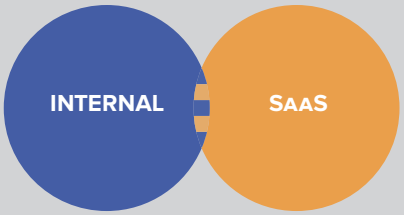
8 PASSWORDS

shared between accounts



7.5 PASSWORDS

are shared between **WORK** & **PERSONAL** accounts



0.8 PASSWORDS

are shared between **INTERNAL** & **SaaS** accounts

Overall, the password related issues responsible for the greatest overall breach risk to the enterprise are:

1. **WEAK AND DEFAULT SYSTEM PASSWORDS** on domain controllers and other infrastructure components and services
2. **CACHED CREDENTIALS** for logging into mission critical systems
3. **PRIVILEGED USER MACHINES** with a high likelihood of breach logging into core servers
4. **PASSWORD REUSE** between work and personal accounts

Balbix®

METHODOLOGY

The Balbix Security Analytics Team randomly sampled data from more than 10,000 users, across dozens of enterprise accounts representing every major industry. This data was continuously collected by sensors, connectors, and collectors deployed across the enterprise network to discover, inventory, and monitor devices, apps, and users across 100+ attack vectors. The near real-time inventory of all IT assets was continuously monitored to identify vulnerabilities and other risk items across 100+ attack vectors, including:

- Unpatched software (CVEs)
- Phishing
- Web and ransomware
- Default, weak or reused passwords
- Encryption issues — missing or improper encryption
- Misconfiguration
- Certificate issues

This data was fed into the cloud-based Balbix Brain, where risk likelihood and impact was calculated for every asset and attack vector, providing a prioritized view of the highest risk issues across the enterprise. That data was randomized, and summarized, in order to generate the credential and password related data published in this report.

BALBIX SECURITY ANALYTICS TEAM

Comprised of Silicon Valley's best data scientists and cybersecurity veterans, the Balbix Security Analytics Team is at the front lines, using advanced AI and ML techniques to work on the most relevant challenges facing the cybersecurity community and our customers. The team specializes in vulnerability and threat research, development of prototype tools, and identification of trends using data science.

Balbix®

I got 99 problems AND THEY'RE ALL RELATED TO passwords

Passwords are an integral component of an organization's security hygiene. However, this is also one aspect that the organization has the least control over. Organizations can enforce policies to generate strong passwords, but this is largely an initiative that is controlled by users.

PASSWORD REUSE

A need for speed in our personal and work lives, coupled with the desire for convenience is at the heart of widely prevalent practice of password reuse. While this may be an understandable human behavior, it is still a problem that organizations need to tackle by making good password hygiene a priority.

In the 80% of data breaches attributable to compromised, weak and reused passwords, the most common attacks leveraged by attackers are password spraying and password replay.

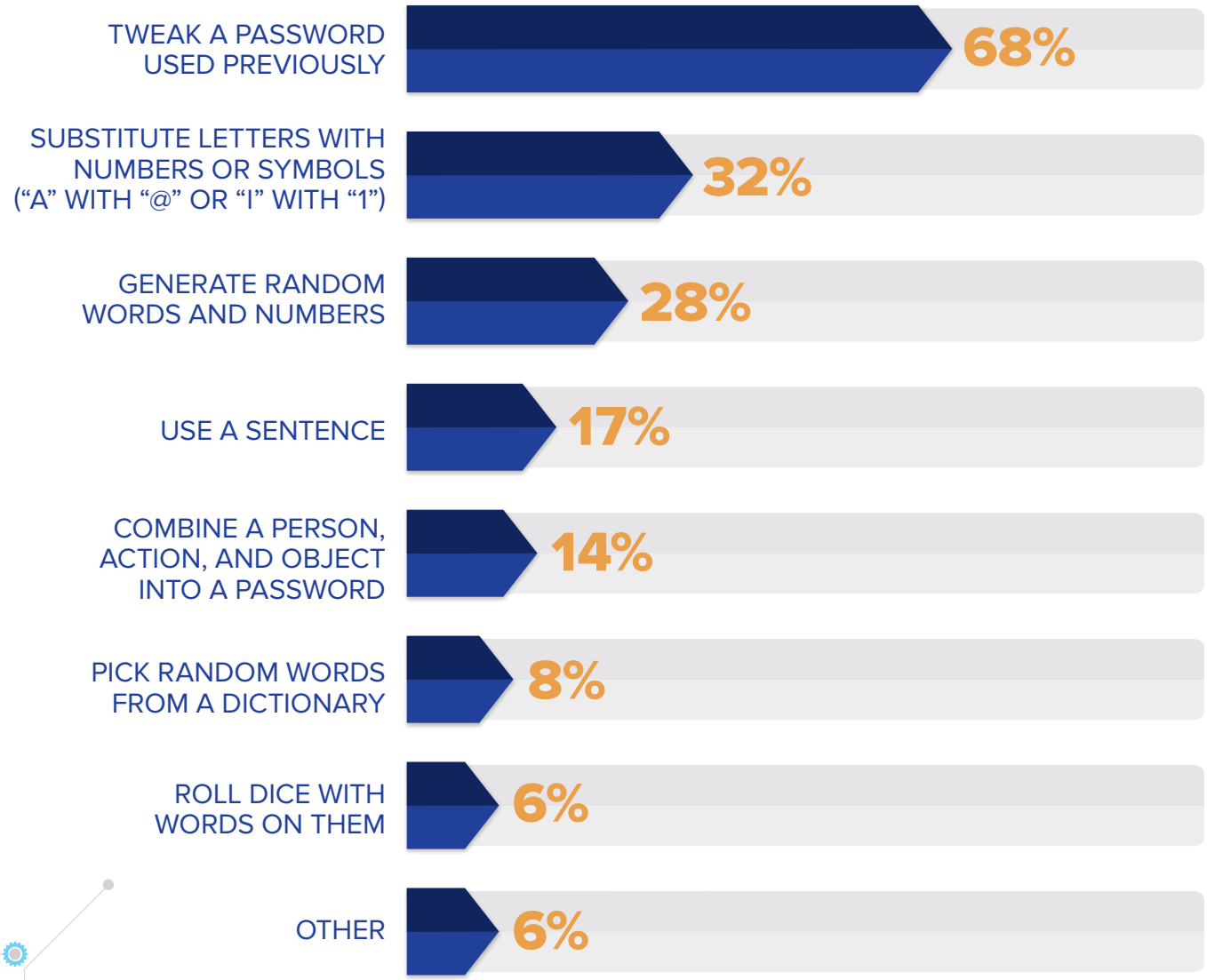
More than 99% of users reuse passwords,

EITHER ACROSS WORK ACCOUNTS, OR BETWEEN WORK AND PERSONAL ACCOUNTS.

Balbix®

HOW PEOPLE COME UP WITH PASSWORDS

A recent survey by **Security.org** found that 68% of people come up with new passwords by tweaking a previously used password.



SOURCE: **Security.org**

Balbix®

PASSWORD SPRAYING

Password spraying is a "type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique, which is leveraged in **40% of Microsoft account compromises**, allows the actor to remain undetected by avoiding rapid or frequent account lockouts." Would-be attackers attempt one password per account, cycling through all targeted accounts, before repeating with the next password. The passwords that attackers use in password spray attempts depends on the type of asset in question.

When targeting end user devices and accounts, such as SaaS and corporate intranet logins, adversaries rely on spraying perennial password favorites, very few of which have changed over time. In 2019, **the top 10 most commonly used passwords** leaked in data breaches were:

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- Iloveyou
- 111111
- 123123

When targeting system accounts and infrastructure devices over administrative protocols such as SSH and Telnet, attackers shift to **passwords commonly associated with such devices:**

- admin
- vizxv*
- default
- 1001chin*
- sh
- 12345
- password
- ttnet
- root
- taZz@23495859*

*Factory default passwords for various DVRs, routers, and other embedded devices

PASSWORD REPLAY/CREDENTIAL STUFFING

Password replay is the second most common technique for credential compromise, and involves taking credentials compromised in one breach, and replaying those same credentials on other sites and applications in an attempt to capitalize on rampant password reuse and lack of multifactor authentication.

On average, a single password is shared across 2.7 accounts.

With over 4 billion records compromised in 2019 across nearly 4,000 breaches, it's safe to assume that your passwords are out there. Balbix found that the average password is reused 2.7 times, and that the average user is sharing 8 passwords between work and personal accounts. This means that every time a password is breached, it's entirely likely that one or more corresponding enterprise passwords have also been breached.

Google studies on password breach alerting indicate that 1.5% or more of all web logins involve known compromised credentials, and of alerted users, only 26% opt to change their passwords when informed that their credentials have been breached. Given this lack of action, multifactor authentication (MFA) is a logical fix. Unfortunately, MFA is used in only **11% of enterprise accounts.**

Why great care and consideration should be taken when selecting the proper password

Credential stuffing —a type of cyberattack where hackers use stolen account credentials, typically found from a breach, to gain access to other sites using the same password.

Balbix®

HIGHEST RISK PASSWORD RELATED ISSUES IN THE ENTERPRISE

Risk originates in many areas, and password related issues are at the top of the list for most enterprises. NIST **advises companies** to verify that passwords are not compromised before they are activated and check their status on an ongoing basis. As the number of compromised credentials expands continuously, checking passwords against a dynamic database rather than a static list is critical.

Here are the four password related issues driving the highest breach risk in Balbix customers, and how to resolve them:

1. **WEAK AND DEFAULT SYSTEM PASSWORDS.** It's all too common to see an old system account with default credentials logging into a domain controller, or an account setup by a vendor that was never removed.

   FIX: Implement policies to change all default system passwords, and to expire passwords regularly. Use MFA whenever possible.

2. **CACHED CREDENTIALS** for logging into mission critical systems. With so many passwords to remember, it's no surprise to find that privileged users are caching credentials in their browsers, even for mission critical systems.

   FIX: Ensure that MFA is used at all times for privileged user logins. Use password manager software instead of browser credential caching.

3. **PRIVILEGED USER MACHINES** with a high likelihood of breach logging into core servers. Risk is transferable. If you have an appropriately locked down critical asset, but that asset is administered by a user on an insecure system, the risk of the locked down asset will be increased as a result of that user administering the system.

   FIX: Ensure that privileged user machines are appropriately patched, with appropriate security software installed. Required MFA for login to all systems.

4. **PASSWORD REUSE** between work and personal accounts. With the average password being shared across roughly 3 accounts, the odds of a successful credential stuffing attack are quite high.

   FIX: Get ahead by requiring enterprise password rotation every 90 days (or more), and requiring MFA for access to any account or application with access to sensitive data.

THE FUTURE OF PASSWORDS

Despite huge investments in user training, tools, and awareness passwords continue to be the Achilles' Heel in most cybersecurity programs, leading to the vast majority of breaches. There aren't yet any complete password replacement technologies on the market, so unfortunately, passwords won't be going away anytime soon. That said, usage will continue to be adapted to make up for the shortcomings of the username and password combination.

Single sign-on, which helps consolidate logins and allows users to remember fewer passwords, will continue to enjoy more widespread adoption, as will the use of password managers. Both technologies allow for users to leverage more complex passwords, without increasing the likelihood of them writing them down or exhibiting other poor behaviors.

Smartphones have also become an important part of many authentication schemes. Initially used primarily as a delivery mechanism for SMS one-time passwords, authenticator applications are taking over as a more secure verification mechanism. Coupled with biometrics tied to the phone itself, such as fingerprints and facial recognition, and the smartphone as an additional factor of authentication has become a powerful tool.

ABOUT BALBIX

Balbix is the world's first cybersecurity platform to leverage specialized AI to provide real-time visibility into an organization's breach risk. The Balbix system predicts where and how breaches are likely to happen, prescribes prioritized mitigating actions, and enables workflows to address the underlying security issues. By using Balbix, CISOs and CIOs can transform their organization's cybersecurity posture, reducing cyber risk by 95% or more, while making security teams 10 times more efficient. Balbix counts many global 1000 companies among its rapidly growing customer base and was named a "Cool Vendor" by Gartner in 2018. For more information, visit our **website** and **blog**, follow us on **Twitter** and **LinkedIn**.