MetaCompliance®

Managing Passwords And Mitigating Password Risk

Passwords have been a mainstay of security since human language evolved. This shared secret can be used to open both physical and digital doors. But like any secret, if it is revealed to the wrong person, it can be used for nefarious deeds.

Passwords offer cybercriminals a way to get past the gatekeeper. That gate is wide open if a password is insecure, shared, or phished. Managing passwords helps to mitigate risk in an organisation. Here is a look at some of the risks of using passwords and tips on managing passwords.

The problem with passwords

Passwords are persistent because users understand them; they are understood by web and app developers and offer basic security. Passwords will persist for these reasons, even with initiatives such as the passwordless system, FIDO.

A password is the most fundamental login credential, but passwords are far from a robust security measure. Because of the doors a password can open, this credential has become a focus of cyber attacks. The 2022 Data Breach Investigations Report (DBIR) identified credential theft as one of the top four methods used to breach data.

The 2022 Annual Identity Exposure Report identified some staggering statistics concerning passwords:

- 1.7 billion credentials (combinations of email address and password or username and password) were exploited by cybercriminals in 2021
- 70% of users were still using compromised passwords a year later
- The number one reused password in cleartext (i.e.unencrypted) was 'password'
- 60% of users reuse passwords. A Google survey found that 52% reuse passwords across multiple accounts
- Only 20% of users have a password manager

The costs of password exposure, theft, and unauthorised access stack up. The 2022 Ponemon Institute Cost of Insider Threats report discovered that:

- The cost of credential theft increased 65% from $2.79 million in 2020 to $4.6 million in 2021/2022
- Containing an insider threat takes around 85 days
- Incidents that took more than 90 days to contain cost, on average, $17.19 million

How passwords end up in the hands of cybercriminals

Some of the most typical ways that passwords are stolen or compromised include:

Malware infection
Malware designed to steal data will send any password/username/email combos input by a user to the cybercriminals controlling the malware.

A SpyCloud report found that in 2021, "RedLine Stealer" malware was widely used to steal credentials and other data from Windows users. The malware was available for purchase on a dark website for $800 or a malware-as-a-service subscription for $200 a month.

Data breach
Data breaches offer a cybercriminal a way to access stolen passwords and username or email pairs, i.e. login credentials. For example, the Collection 1-5 data breach of 2019 exposed 2.2 billion passwords and email addresses.

Data breaches typically occur via unauthorised access to a database, a security misconfiguration that leaves

the database vulnerable, accidental exposure from email mis-delivery, or deliberate hacking. In a cycle of cybercrime, a compromised database then releases more login credentials to carry out further attacks.

Phishing
A popular way to steal passwords is phishing. In fact, the 2022 DBIR noted phishing as one of the top four data breach methods. Spear-phishing is a particular issue for system admins and privileged users targeted for their privileged access credentials.

Third-party vendors are targets in password-related attacks. For example, in the case of the Colonial Pipeline ransomware attack of 2021, a single stolen password from an ex-employee was linked to the attack that caused half of the USA's fuel supplies to be temporarily closed.

Accidental exposure and insider threats
Employees like to share passwords with colleagues as well as reuse them. A recent survey found that almost 42% of employees share passwords with co-workers. The same study found that 1 in 4 employees still had access to old accounts even after leaving a company.

Accidental password exposure or unauthorised access is a significant contributor to cyber attacks and data breaches, with the 2022 DBIR finding that 82% of attacks involve a human being.

Five quick tips to managing passwords

Here are five tips for managing passwords and reducing risk:

Set up and enforce password policies
Password policies are the first step in de-risking the use of passwords. Password policies include everything associated with managing passwords and keeping passwords secure. For example, a policy should include the safe storage of passwords and how often a password needs to be changed.

Password policies should also clearly state how employees should create and manage passwords. Policies should be distributed to employees, and management of the policy should be automated across the policy's lifecycle to ensure it is accepted and understood across the business.

Use a password manager
Password managers reduce password fatigue and, therefore, can help eliminate password reuse and sharing. If you're using a password manager, then technically, you only need to remember one set of credentials—the master password to log into your password manager.

Once you're logged into password manager using your master password, the password manager does the rest – stores, generates, and updates passwords.

But password managers are still underused in companies. There are lots of password managers, but cloud-based services can be easier to deploy and administrate. Look for a password manager that can also work across operating systems and protects other data types, including passwords.

Use a second factor (2FA/MFA)
Using a second factor, such as a mobile authentication code, is a useful way to add another layer of security to the access of an application. However, you should not rely on 2FA to offer 100% risk-free access control.

Cybercriminals are already working out ways to circumvent second-factor authentication. If you can, implement 2FA, but back this measure up with our following two tips to de-risk passwords.

Train employees about password hygiene
Password policies should reflect the cyber security industry standards for creating, using, and managing passwords. However, enforcing this policy requires employees to understand why password hygiene is essential and how to keep passwords secure.

Cyber Security Awareness Training programs typically include modules on creating strong passwords and keeping passwords secure.

Use phishing simulations to reduce password theft
Phishing is one of the main methods to steal passwords and other credentials. By training employees in how phishing works and what the tell-tale signs of a phishing message look like, a company can help prevent the theft of credentials via phishing.

Phishing simulation platforms offer a centralised and configurable way to send out simulated phishing messages to staff. An advanced simulated phishing platform will also allow you to tailor the simulated phishing messages to reflect the different roles in your company.

Organisations will likely continue to use passwords for a while to come, adding to the risk of a cyber attack. However, by applying the five tips outlined here, you can de-risk the use of passwords by your employees. These tips help prevent data breaches and ransomware infection and help your company comply with data protection regulations.

About the author

James MacKay is the COO of MetaCompliance and a recognised Security Awareness Training expert. James has a deep understanding of delivering effective training and is committed to helping organisations keep their staff safe online, secure their digital assets and protect their corporate reputation.

Third Floor, Old City Factory,
100 Patrick Street, Londonderry BT48 7EL
t: +44 (0)28 7135 9777 e: info@metacompliance.com
www.metacompliance.com

MetaCompliance®