



eBook

SIMPLIFYING PASSWORD MANAGEMENT

How to Get More Control
and Better Security without
the Headache

INTRODUCTION

Passwords...we can't seem to live with them—and we certainly can't live without them.

Much like a combination to a safe, passwords guard our valuables. Strong passwords act as a digital self-defense to protect confidential, sensitive, and proprietary information.

Even though we all know how important passwords are, it doesn't seem to make it any easier for us to follow through on all the password security best practices.

But the threat is real. Hackers are getting more sophisticated, and they love going after passwords. It's the easiest way they can evade detection when getting into your systems and accounts. In fact, nearly half of all data breaches involve stolen passwords. (Source: [SMB Guide](#) and [Verizon](#))

The threat from inside is real, too. We're human. We forget passwords, make them too easy to crack, use variations of the same password, and somehow think we're not important enough to be a target for attack. But criminals don't think like that.



SNAPSHOT OF POOR PASSWORD PRACTICES:

- The most popular password in 2023 was 123456 ([SMB Guide](#))
- 37% of workers have used their employer's name in an office-related password. ([Keeper Security](#))
- More than 9 in 10 IT leaders have serious concerns about user-generated passwords and are also worried about passwords being stolen (source: [TechRepublic](#) and Ping Identity)
- 3 in 4 people say they've been locked out of an account after forgetting their password ([SMB Guide](#))

What can we as IT leaders do to help? As one of the first lines of defense, it's critical to face known password problems head-on, help everyone ensure passwords are as strong as possible, and minimize all the ways passwords can fall into the wrong hands. **Let's get started.**

WHAT YOU'RE UP AGAINST:

Common Employee Password Missteps

Only 31% of organizations use a password management tool. The rest rely on stone-age password management techniques:

- 42% use sticky notes (which can be stolen)
- 59% use human memory (which can be forgotten)

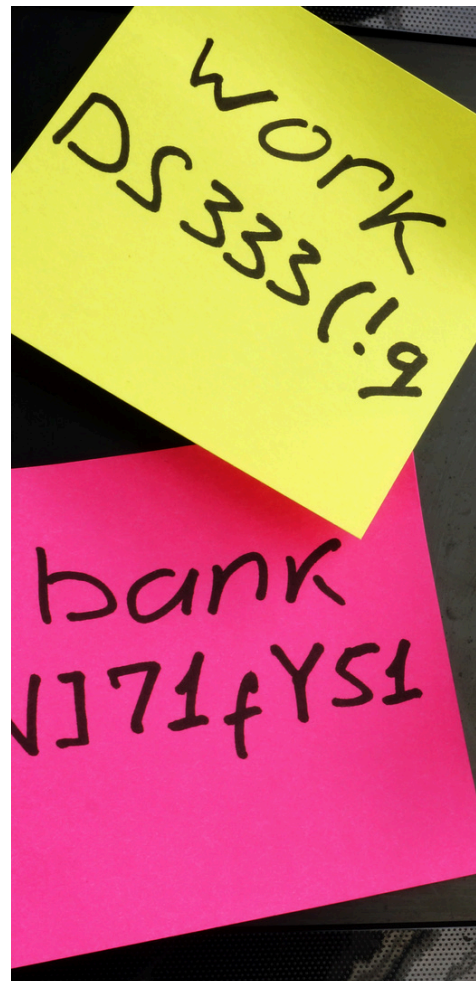
Source: [Ponemon Institute State of Password and Authentication Security Behaviors Report](#)

Good intentions, bad outcomes

It is widely estimated that the average person has to remember more than 100 passwords! No wonder why they are looking for some relief. Consequently, the following employee missteps frequently occur in the workplace:

•➔ **Bad password hygiene**

Despite the best of intentions to create strong passwords, employees may take shortcuts and use fewer characters than recommended or use personal data that's easier for them to remember.



- Employees use weak passwords like ilovecoffee and 123456
- Favorite passwords are reused for multiple logins
- Passwords remain the same—for years—even if a data breach is announced

These passwords are simple to hack and expose your organization to significant risk. You'll never achieve the highest level of security if your first line of defense is weak.

•➔ **Forgetting passwords**

Password resets are a nuisance for everyone. Employees are reeling from password fatigue and simply can't remember hundreds of unique passwords. As a result, IT departments and MSPs are called to help. Unfortunately, just one password reset can:

- Drain IT resources
- Negatively impact employee productivity
- Cost the company money

•➔ **Sharing passwords with coworkers**

Employees mean well. They want to empower coworkers to access shared accounts when they need to get the job done. Though sharing a password to the company LinkedIn page with your fellow marketing department team members may seem like a reasonable request, it puts sensitive information at risk. Consider the fall-out if:

- Cybercriminals intercept credentials shared on unencrypted platform, change your credentials, and lock your company out of the account.
- A disgruntled employee sees a sticky note with the password, logs in, and posts something that negatively impacts company image and credibility.

WHAT WE CAN DO TO IMPROVE EMPLOYEE PASSWORD GENERATION AND MANAGEMENT

To combat an evolving threat landscape, it's important to stay informed about the latest security trends. Organizations should provide training and resources to employees about password security on a regular basis to address issues like password strength, the dangers of phishing and social engineering, and practical ways to safeguard sensitive data.

It's also important to educate your workforce about how to report and address potential security breaches. Preserving the integrity of your organization's systems relies on an effective combination of password strength, breach awareness, and swift incident response.



THE ANATOMY OF A STRONG PASSWORD

Share these tips with your workforce to strengthen and maintain your organization's password security. Passwords should be:

- **Long and complex.**

Choose an unpredictable password that is at least 12 characters long and includes a mix of special characters, numbers, and symbols.

- **Unique.**

Create a unique password that does not use personal or company identifiers or elements of previously used passwords.

- **Exclusive.**

Don't use the same password for multiple accounts.

- **Multi-layered.**

Do use multi-factor authentication in combination with your password to verify user identity. It can be a code texted to your phone, a biometric, or randomly generated code via an authenticator app.

- **Securely Managed.**

Access, share, and securely store passwords with end-to-end encryption and built-in guardrails to ensure you follow password best practices.



WHY BOTH IT PROS AND EMPLOYEES NEED A PASSWORD MANAGER

Isn't it easier to do things when you have a little help from friends you trust?

Password managers play an important role in your organization's cybersecurity strategy. And we know from experience that foundational security works best when you've protected all the entrances and plugged all the holes.

Give your employees a helping hand

For employees, password managers act as a user-friendly way to enforce password best practices across your organization and protect against threats from cybercriminals. They are effective at reducing stress for employees who frequently forget their passwords and provide an instant boost of strength to those who were just using 123456 for every login.



Here are some of the instant security and productivity boosts for employees:

- Long, complex, unique, exclusive passwords are generated and stored for every login credential needed
- Encrypted copy of all password data is protected by one master password
- See which passwords need updating at-a-glance
- IT can help restore access quickly if needed
- Safe password sharing is enabled allowing the ability to grant access to accounts for a specified time period and without revealing the actual password

Give yourself added support in the fight to protect accounts

As an IT professional, time is precious, and you could use all the help you can get. Password managers offer an easy way for clients and team members to keep better track of passwords and maintain compliance with organizational security policies.

Think of a password manager as both an assistant and an enforcer in your fight to strengthen security and minimize risk.

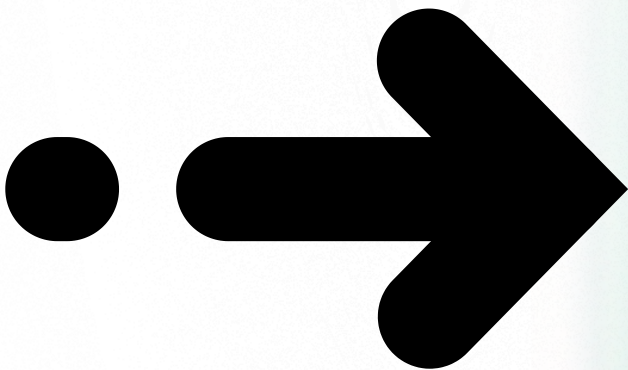
With an end-to-end password manager by your side, IT professionals can:

- Monitor passwords in one place – making it easy to identify stolen passwords and make changes to enhance security
- Assist employees with secure password sharing and revoke access when no longer needed
- Gain visibility into password security across the organization through dashboards, usage logs, security scores, and reports
- Easily add and remove users to your account
- Access and manage permissions for client passwords based on role-based assignments
- Protect employee password information with an encrypted storage solution

SAFEGUARDING PASSWORDS: SECURITY FEATURES YOU NEED IN YOUR PASSWORD MANAGER

Are you ready to add a password manager to your organization's cybersecurity strategy? Smart move.

Before you onboard the first inexpensive password management solution you can find, it's important to do your homework. Not all password managers are created equal.



Here's what you need to look for:

- ✓ **Strong encryption practices.**

All data stored in the password manager should be encrypted, not just the passwords themselves.

- ✓ **Enterprise grade security.**

User data should be encrypted, with a unique key, and never stored locally or on servers.

- ✓ **Secure cloud back-ups.**

Cloud back-ups should be saved to a secure cloud storage location.

- ✓ **Compatible with MFA or Single Sign-on (SSO).**

Every solution works best when layered with other security practices. It's critical your password manager can work with MFA and SSO solutions to protect your master password.

- ✓ **Protects data from theft.**

What happens if an employee device is stolen or misplaced? Look for solutions that offer a remote delete function that can automatically delete encrypted user data if someone tries to access the password application.


HOW TO USE PASSWORD MANAGEMENT AND PAM TOOLS TOGETHER TO STRENGTHEN SECURITY

Privileged access management (PAM) is one part of a comprehensive security strategy that focuses on controlling the access and permissions for users, accounts, processes, and systems throughout an IT environment. Effective password management supports this effort by preventing unauthorized privileged access to critical systems.

What are the benefits of using privileged access and password management solutions together? Here are just a few:

- ➔ **Minimizes risk of stolen credentials and data breaches**
- ➔ **Secures sensitive company data**
- ➔ **Provides more control over user privileges**
- ➔ **Protects passwords with roles-based access and secure sharing**

CONCLUSION



Cybercriminals are relentless—and we're human! It's easy to become numb to the constant threat of stolen data and system breaches.

Be vigilant in the fight to protect privileged access and passwords! Get everyone on board to help prevent entry into your systems by:

- Educating your workforce about the importance of strong passwords
- Sharing tips to shut down phishing and social engineering attacks
- Encourage the proactive reporting of suspicious activity
- Using many layers of security to protect passwords and other sensitive data

Password Boss WebApp provides industry-leading password protection built specifically for organizational use. Don't let password stress get in the way of your security. Learn more at cyberfox.com/passwordbosswebapp.