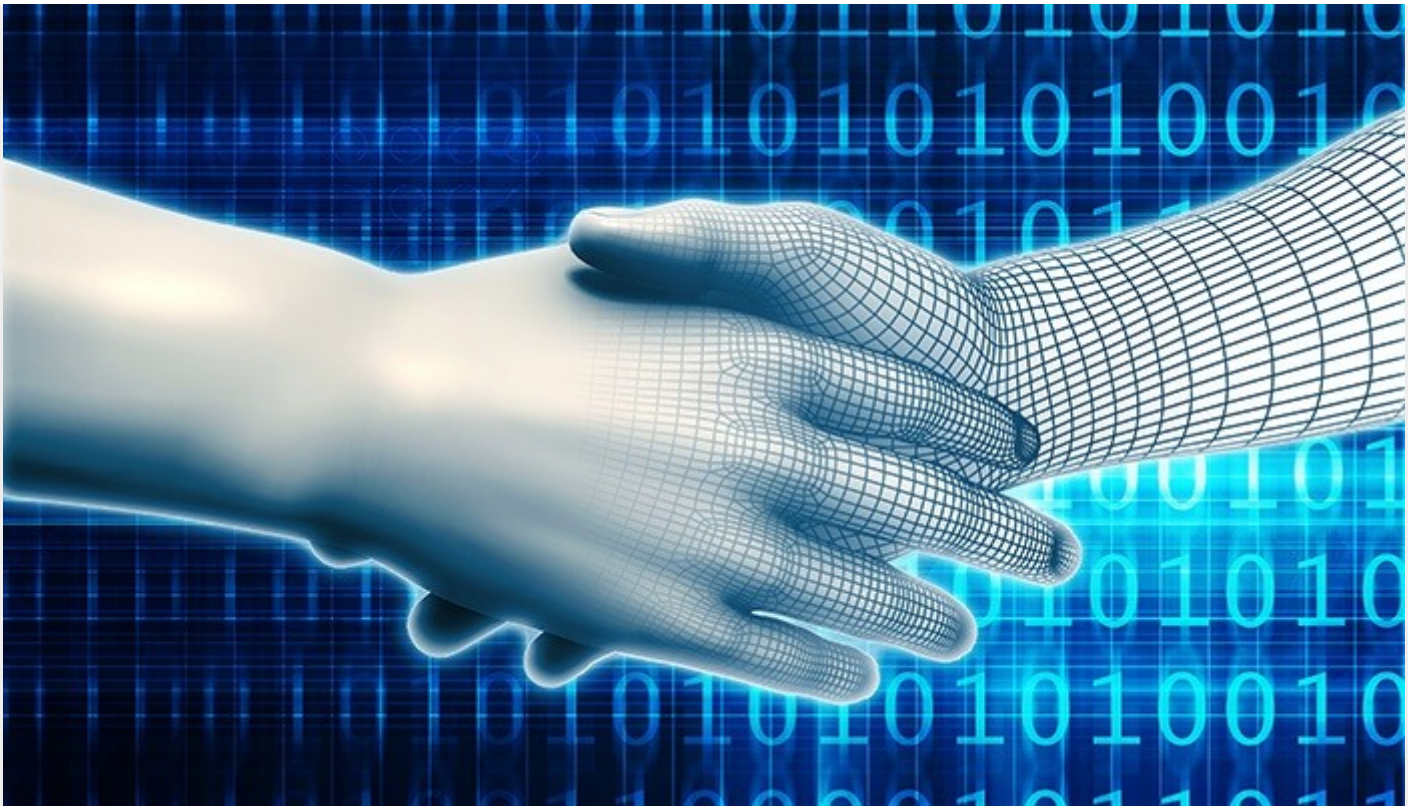
# ENTERPRISE PASSWORD MANAGEMENT BEST PRACTICES



Choosing a password for an account used to be easy. Take your pet's name, add an anniversary or birthday year, and voila. Then, repeat that password or a close variation of it for memory's sake.

Unfortunately, with Facebook's data leaks and hacks into many companies, from Equifax to LinkedIn, we should be paying more attention to passwords. We know password best practices — keeping a unique password for each account, using random words, and changing them often — but most of us aren't doing this.

For companies, however, password management is critical. Weak passwords can expose vital company data and proprietary information to hackers around the world. Companies urge their employees to follow the same best practices as individuals should when it comes to password management.

But recent research shows that these tools aren't necessarily helping. In fact, they may be hurting your company's security. Instead, security experts are suggesting new practices, some that are contrary to traditional password hygiene and others that move the onus from the employee or end user and place it squarely with the company. Let's take a look.

## Current password management isn't working

We already know that each password should be long, random, and, ideally, unique to every account, which can easily total dozens. At work, you may have anywhere from one to twenty more passwords

to remember – and that is difficult. A person who changes and remembers every password every month, as best practice dictates, is equivalent as trying to remember a new 660-digit number.

The problem with reusing passwords or sticking to common words is that they are much easier to hack, and hackers around the world are trying. So how should companies handle password management? And how much is the responsibility of employee?

Cybersecurity is often driven by fear. Experts warn, however, that fear-driven practices aren't helpful, suggesting that companies instead consider data related to cybersecurity. HaveIBeenPwned is a popular website that tracks email and company-level hacks around the world. This data compilation alerts users when and where their emails, and other personal data, were hacked. For example, the password "123456" has been hacked at least 23 million times.

When companies force employees to change their passwords monthly or quarterly, they may actually be contributing to unsafe passwords.

This brain exhaustion results in most users opting for the easiest route, which results in weak passwords. Such passwords don't meet necessary security levels, relying on common words and substituting numbers for letters (A = 4, E, = 3, O = 0, etc.), so hackers can get in with unsophisticated brute force attacks.

Security experts warn that companies must stop blaming employees for password insecurity. Instead, companies must improve their infrastructure. Then, companies should arm their employees with the necessary information to make decisions.

As an example, if one employee already deploys a password management system that creates long, complicated, random passwords for each account, that password is significantly less likely to be hacked – so why force that employee to change passwords?

## Best practices for company password management

Healthy company password management must incorporate two strategies: a top-down, infrastructure approach and an employee-level approach.

Here are common ways companies can improve password management from the top down:

- **Minimize your system's use of passwords.** Consider alternatives to multiple passwords by using single sign on systems or password synchronizations. Add passwords only to systems that require secure access.
- **Blacklist common password choices.** Start with the 100,000 most commonly hacked words from HaveIBeenPwned.
- **Monitor and notify users of strange login attempts.** Informing employees of successful and unsuccessful logins means they can inform the company if any attempts were not their own.
- **Lock accounts after 10 password guesses.** This defends against brute force attacks.
- **Require employees to change passwords only if you suspect it's been compromised.** Unnecessary password changes result in weak passwords.
- **Provide employees a way to manage passwords.** Whether physically, in a super-secure filing cabinet, or digitally, with password management software such as LastPass, Keeper Business, or Dashlane Business. (You may already use software that includes these services.) Though these digital solutions may be targeted by hackers, they are much more difficult to hack because users only need to remember a single, unique password.

- **Prevent shared passwords.** Systems that are used rarely often have a single password that employees share, which is risky. Instead, deploy hardware tokens like RFID badges.
- **Keep software updated.** Vital security patches are common in software updates.
- **Change default passwords before deploying systems.** New software often comes with a standard password like "password1" or "User1" that are easy to hack.
- **Search for plain-text passwords in employees' files.** Employees often save a document or email with their work-related passwords in plain text. These files are easy to find with a few standard searches. If an employee is using this method, the text must be encrypted.

With a top-down strategy in place, companies must also communicate best practices directly to users, which can apply both for company-related and personal accounts:

- **Build password awareness.** Explain your company's new password management strategy: all the top-down steps you've taken and the new requirements for employees. Employees are more accepting of change when they understand the reasons – and you've given them both the ability and the responsibility to choose better passwords.
- **Encourage specific types of passwords.** Security experts encourage stringing together four random, uncommon dictionary words or using a pattern such as CVC-CVC-CVC-CVC for consonant-vowel-consonant.
- **Pay attention to encrypted websites.** Users should never enter passwords or personal information into websites that aren't encrypted. Encrypted sites are indicated by a lock icon located in the browser's search field; without it, assume the website is unencrypted.
- **Lock computers screens.** This ensures only that approved employee is accessing allowable systems.

Regularly reminding users of good password management should no longer be your company's first line of defense. Instead, with company-level and employee-level best practices in place, regular reminders serve as the final, good measure step towards password safety.