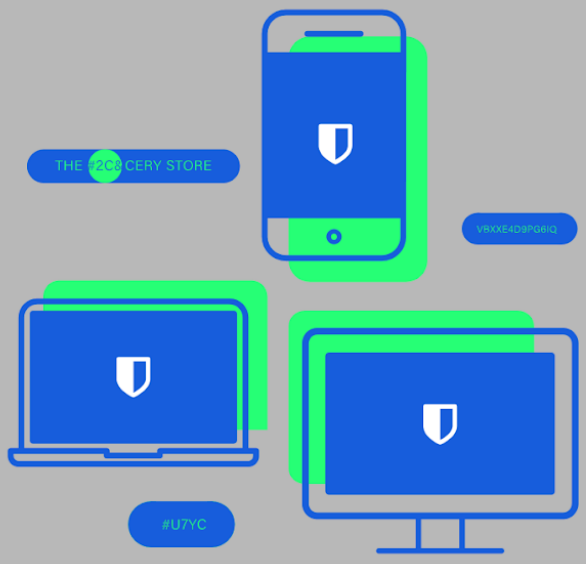

Five Best Practices for Password Management

bitwarden

While organizations continue to make security a priority, an important part of that effort involves educating and empowering general users about best practices.
Consider some of these statistics from the Yubico 2019 State of Password and Security Authentication Security Behaviors Report:

- 2 out of 3 respondents share passwords with colleagues
- 51 percent of participants said they reuse passwords across personal and business accounts
- 57 percent said they did not change their passwords after experiencing a phishing attempt

To bring change at an organization, security and IT teams must educate employees about best practices. In regards to password management, one of the easiest ways to encourage good password hygiene is to deploy a password management solution across your workplace. Here are some other best practices to adopt.

1. Leverage a password management solution.

Throughout the day most people visit many different sites that require passwords. Memorizing tens of unique and sufficiently strong passwords (or passphrases) is virtually impossible. A password manager simplifies password use across different sites to keep users more secure.
There are a number of solid password managers out there. Prioritize those that work cross-platform and offer services for individuals for free or at least, at a very low cost. Most password manager capabilities have also expanded over the years.

2. Choose a tool that you can easily deploy across your organization.

Password managers need to be easy-to-use for every level of user–from beginner to advanced. When considering a large or distributed employee-base, the applications should be user intuitive and easy to deploy. For example, whether you choose the Bitwarden Cloud or deploy your own self-hosted instance, getting Bitwarden up and running is easy. And Bitwarden Directory Connector works with today's most widely used

directory services such as Azure, Active Directory, Google, Okta and others, to keep your Bitwarden users in-sync with your teams and employees.

3. Only change passwords when you might have been compromised.

The days of changing your password every three months are over. You should now only change them if you think you've been compromised. The National Institute of Standards and Technology (NIST) doesn't recommend users change passwords frequently. This actually leads to behavior that may result in weaker passwords over time. You can determine if you've been compromised by referencing tangible evidence, such as credit card fraud, or using a tool like your password manager that can tell if your password was exposed in a breach.

4. Use strong, unique passwords.

Using strong, unique passwords for every service you use online helps minimize the impact of data breaches. A strong password doesn't necessarily mean just adding special characters or numbers to a common word or name, it means increasing the password's entropy, or randomness. One easy tactic for creating a strong password is to use a passphrase. A passphrase combines seemingly unrelated words or phrases that are easily memorable to the user but would otherwise be hard to guess by an attacker. Passphrases have a high degree of entropy while also being easy to remember.

5. Enable two-factor authentication whenever possible.

With two-factor authentication (2FA) becoming more common across consumer and business websites, good password managers should include ways to expand on this function. Using 2FA increases the security of your account by requiring you to enter another token beyond supplying your master password. Even if someone were to discover your master password, they could not log into your password manager without access to the additional token.

If you'd like to get started with a password manager, you can sign up for a free Bitwarden account here.