RESOURCE CENTER

# Small Business Password Management

Get the full interactive view at
https://bitwarden.com/resources/password-management-small-business/

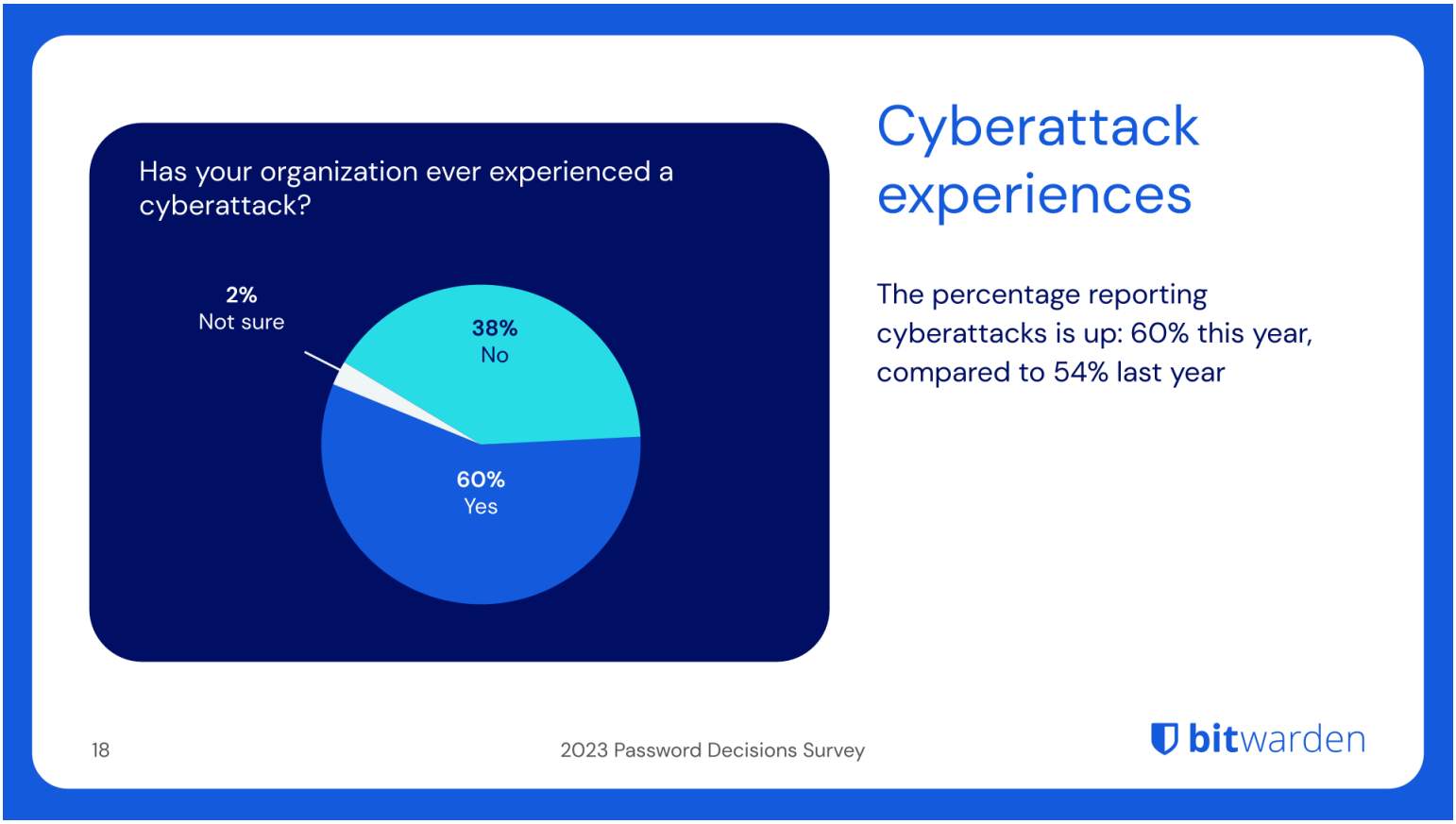
bitwarden

## What is small business password management and why is it so important?

Most data breaches covered by the media become international news because they deal with global organizations or large well-known enterprises. However, small and medium businesses (SMBs) have most of the same challenges and concerns around data security that enterprises do—just on a smaller scale. They're also working with smaller budgets and smaller IT teams (if they have in-house IT expertise).

While corporate data from the world's biggest enterprises might be the most attractive target for many hackers and other malicious actors, SMBs are still at high risk of ransomware, data theft, phishing attacks, and much more. According to a recent Cumulus Global report, 43% of small and medium businesses have been the target of a cyber attack. Why? Hackers often view SMB data as "low-hanging fruit" because they assume smaller businesses don't have the robust security or protection that big corporations can afford.

No matter how small your business or your security budget, there is a lot you can do to protect your company data—and it all starts with **passwords**.




Slide 18, 2023 Password Decisions Survey

"My pick for best password manager easily belongs to Bitwarden — not only because it's open-source, but because it offers a perfect blend of simplicity and advanced features."

**TechRepublic**

43% of small and medium businesses have been the target of a cyber attack

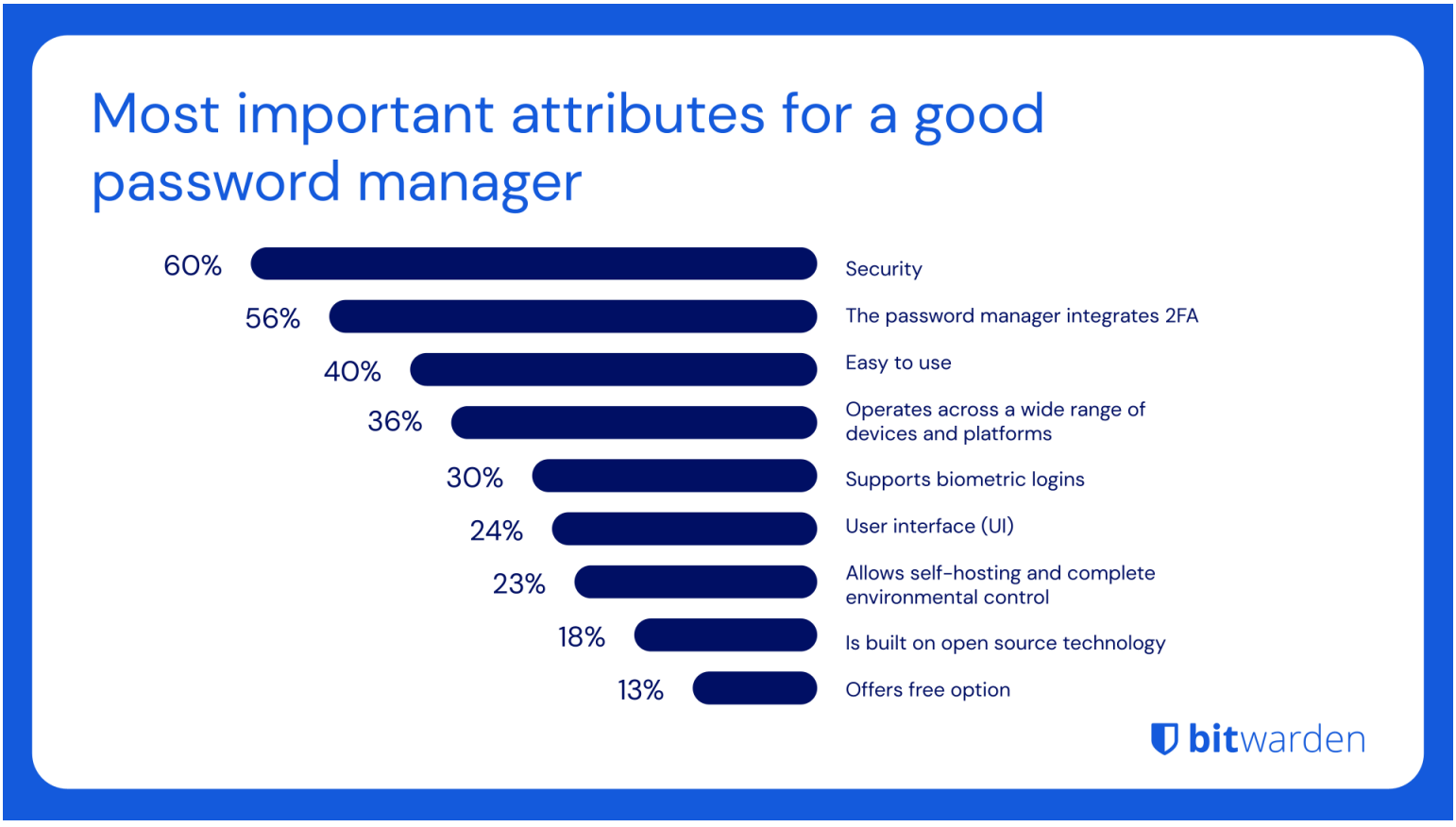
Cumulus Global report

## How password overload leads to increased security risks

Today, web users need a password for practically every site they visit online, and every application they use in their daily work. The issue with needing so many passwords is that it's impossible to remember them all. People will use the same password or a small collection of passwords across dozens or even hundreds of online accounts to overcome that challenge. Reused passwords also tend to be ones that are easy to remember by using personal information, such as birthdays, anniversaries, or the names of children or pets.

It is so risky to reuse easy-to-remember passwords because hackers can easily gain access to that information through social media sites. And by reusing passwords across multiple sites, hacker computers can brute-force one account password and then use that information to gain access to all other accounts with the same credentials.

The key takeaway is that passwords are big business for hackers. In fact, a majority of data breaches and security incidents are caused by threat actors gaining access to weak passwords. Business and personal email account passwords, for example, are particularly desirable to hackers because they can use your email to reset passwords on other sites and gain access to confidential documents without your knowledge. The solution is to take password management seriously by making it part of your overall business security strategy.




Slide 7, 2023 Password Decisions Survey

## Why business password managers should be a critical part of every SMB security strategy

A password manager is one of the best ways to protect your entire company from password theft or misuse. Password managers are computer programs that store, encrypt, and manage login information for users, including usernames and passwords. They can log you into those sites and applications automatically and keep them protected from hackers. A single master password is typically used to get into the password database, so that's just one password to remember. A password manager will also help you generate strong, unique passwords that aren't based on personal information. Because the password information is stored and managed in a central repository, you can access it on virtually any device you use, whether it's a desktop computer, laptop, smartphone, or tablet.

With a small business password manager, everyone in your company is freed from having to remember their login information for every single website and application they use. The way it typically works is, when you visit a website, instead of typing a username and password into the site's entry screen, you can simply type your master password into the password manager. The password manager system then automatically enters the website login information for you. With your master password, you can easily and efficiently access every account or website you have. Passwords aren't the only information you can store, either.

Small business password managers can also store other private data, such as corporate credit card numbers. The applications can also protect against phishing in cases where you accidentally mistype a website name and go to a fake site operated by a malicious actor. Say you wanted to log into your bank account at citibank.com, but in your hurry you typed citibnak.com. If a hacker had set up a phishing site at the misspelled site, you might think you were on a legitimate bank site. Without a password manager, you might try to log in with your username and password—and now the hacker has that information. A password manager, however, would detect the misspelled URL and not enter your login information, alerting you to the problem.

## Why relying on your browser-based password manager is risky

Most of today's web browsers, including Chrome and Firefox, have built-in password managers, but they don't compare to the protection and security of a dedicated application. Here's why:

- Some browsers don't encrypt your password data, leaving that information easily accessible to anyone who knows where to look.
- Browser-based password managers are designed for individual use, which means they don't support the sharing of credentials among work partners or teams.
- Browser-based password managers lack important features such as password generator, and cross-platform support, meaning you won't be able to access passwords on all your devices.
- For businesses, the ability to log events and conduct audits is important. Browser-based password managers don't provide these capabilities.

## The benefits of using a password manager for SMB security

- No more passwords to memorize—just a single master password.
- Your passwords will be highly secure and unique across every site, application, and user.
- Access passwords and other secured data from practically anywhere, on any device; this is especially beneficial for remote workers and employees who travel from site to site.
- Save time with auto-filled login information; some managers can also auto-fill other data such as name, address, phone, email, and so on.

- Protect your company and personal data; with strong unique passwords, your accounts are essentially siloed from each other, so if a hacker gets into one, they don't get into everything.

## Important considerations when choosing your small business password manager

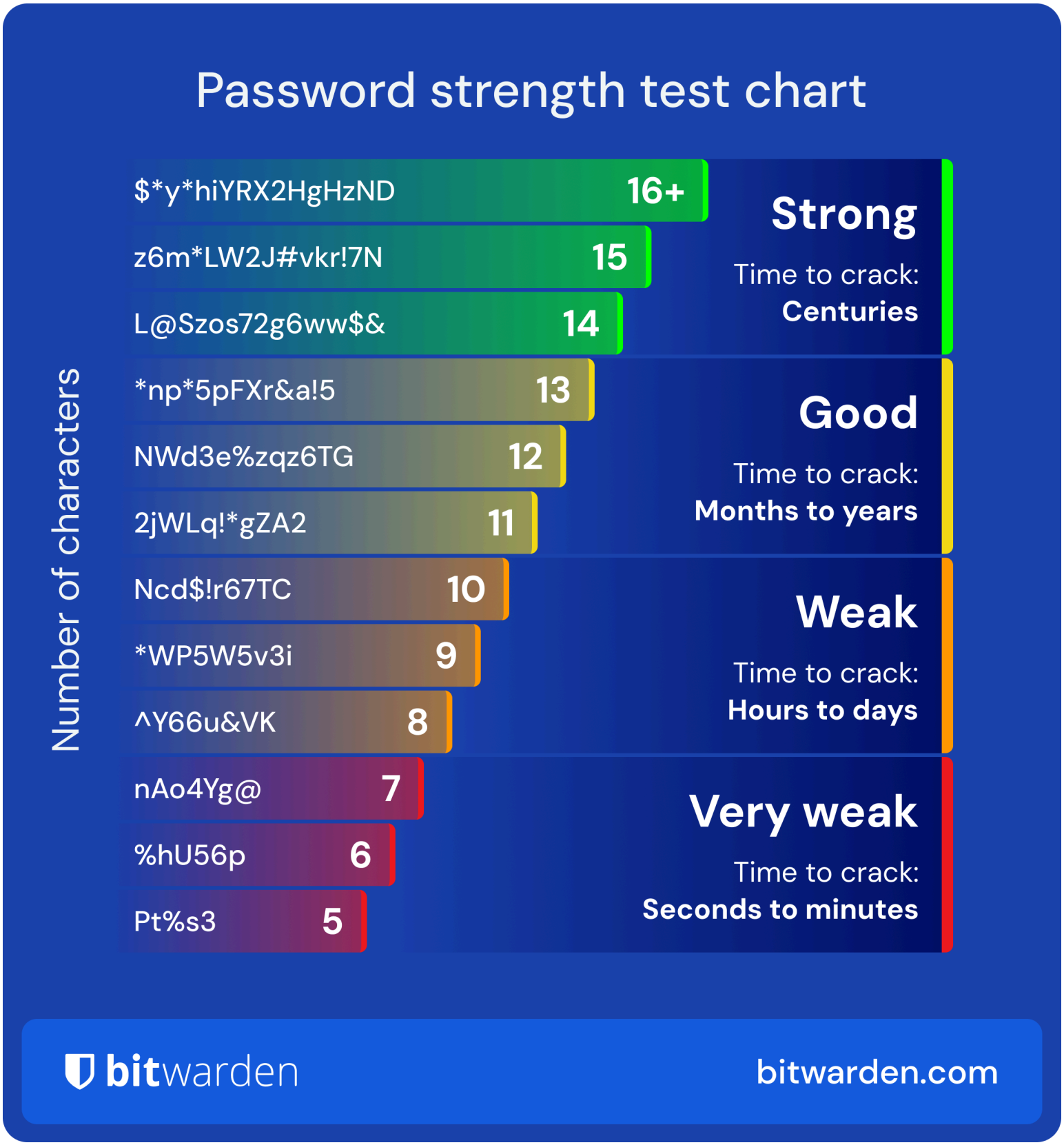
Based in the U.K., the National Cyber Security Centre (NCSC) has some recommendations for SMBs that want to improve password security and are looking for a password manager. The two most important things you can do to protect company data are:

1. Use a **strong, unique password for your email**—using three random words, for instance.
2. Turn on **two-step verification** for your email, so you will use a password and then a secondary identification, such as a code you receive by text.

When selecting a password manager for your small business, be sure to find one that makes it effortless to create strong, unique passwords for every account; supports two-step verification; streamlines and simplifies the backup of all stored passwords and other data.

Other considerations for choosing the best small business password manager include the following:

- **Ease of use.** Because everyone in the company will use it, your password manager should be simple and user-friendly. The application won't help if people don't use it.
- **Integration.** A password manager that doesn't interoperate with your existing IT infrastructure won't be of much use. SMBs typically have small IT teams if they have them at all, so whatever helps streamline management and operations is a plus.
- **Simple admin management.** Administrative controls are important, and a password manager shouldn't add complexity to IT's workload.
- **Reporting capabilities.** A good password manager will provide a variety of report options that allow you to gain insight into adoption and usage across the company and any issues to address.
- **Compliance support.** As industry and governmental regulations continue to evolve around data security, it's important to be able to set policies within the password manager to monitor that users are staying compliant.




**Why Bitwarden is the top business password manager for SMBs**

In July 2022, TechRepublic named Bitwarden the "Best Password Manager for SMBs." TechRepublic writer Jack Wallen said he ranked Bitwarden as number one “not only because it’s open-source, but because it offers a perfect blend of simplicity and advanced features. Bitwarden works incredibly well on every platform and every browser.” Even on the free tier, he said, “you still get unlimited passwords and just enough features to make Bitwarden a perfect platform for those new to using a password manager.”

Trusted by thousands of businesses and millions of end users globally for secure password storage and sharing, Bitwarden allows SMBs to store logins, secure notes, and more; collaborate and share securely across teams and departments; and access login data anywhere on any device.

As Wallen mentioned, the Bitwarden commitment to open source software makes the password manager a leader in trust and security—especially because Bitwarden source code can be inspected and reviewed by anyone. This means businesses don’t just have to trust that the software is secure; you can inspect the code to verify that yourself. Bitwarden also participates in an independent security researchers program and regularly employs third-party auditors, such as Cure53, for penetration testing and official security assessments.

The open source nature of Bitwarden paired with industry-leading security protocols such as end-to-end AES-256-bit encryption, salted hashing, and PBKDF2 SHA-256 sets Bitwarden apart from other solutions. Bitwarden seals your data with zero-knowledge encryption before it ever leaves your device, and only you have access to it. Not even the Bitwarden team can view the private information stored in your vault.


## How to get started with Bitwarden

**Step 1.** Choose the plan that best fits your business (or personal) needs.

**Step 2.** Start your free 7-day trial and **remember to store your master password in a safe place**.

**Step 3.** Explore the download options to access your Bitwarden vault across all preferred browsers and devices.

Have questions or need assistance? Contact sales to get more information on features, pricing, and deployment options.