THE BEST PASSWORD MANAGEMENT GUIDE

brightflow
TECHNOLOGIES

The Best Password Management Guide: Everything You Need to Know

Weak passwords are the primary gateway that hackers exploit, and if not meticulously crafted and managed, they pose a substantial risk to both you and your business. Even if you follow the best cybersecurity practices, have premium antivirus software, or possess knowledge of cybercriminal tricks, weak passwords can nullify all your efforts.

It's alarming how swiftly hackers can crack weak passwords using automated tools; Alex Balan, the director of security research at Bitdefender, notes that a hacker can decipher an 11-character password comprised of numbers in just *two seconds.*

However, the good news is that by embracing stronger password practices, you wield the power to significantly enhance your cybersecurity defenses. Your commitment to robust password management is a pivotal step towards safeguarding your digital assets and thwarting potential threats.

In this guide, we'll make a complicated subject easy to understand by breaking it down into three digestible chunks:

- Understanding Weak Passwords
- Creating Strong Passwords
- Essential Cybersecurity Tips

Understanding Weak Passwords

Did you know that 81 percent of hacking-related breaches occur due to stolen or weak passwords? Weak passwords are more common than you'd think.

The most common passwords are, coincidentally, the easiest to guess.

Many people make easily guessable passwords because making and memorizing multiple passwords can be challenging.
For example, the five most popular passwords globally, according to GitHub, are:

123456 | Password | 12345678 | qwerty | 123456789

It's equally concerning that Google found that almost a quarter (24 percent) of Americans have used weak passwords like "abc123," "Password," "123456," "Iloveyou," "111111," "Qwerty," "Admin," and "Welcome."

These passwords offer minimal protection and are then easily guessed by cybercriminals. Google also found that 17 percent of password-guessing attempts were successful among Americans.

Additionally, 59 percent of people use their name or birthdate in their password.

The majority of users polled by Google have included easily discoverable personal information in their passwords such as their name or birthdate. Other common mistakes include using the names of pets, spouses or children.

Creating Strong Passwords

Experts recommend creating unique passwords that include a combination of letters, numbers, and special characters to bolster your security. While complexity is important, the length of your password matters even more.

Our expert advice? Use passwords with a minimum of 12 characters or more whenever possible.

Here's a pro tip: a 12-character password takes 62 trillion times longer to crack than a six-character password.

Adding each character significantly increases the difficulty for hackers to crack the password.

According to a Scientific American article, a six-character password with lowercase characters provides approximately 3 x 108 possibilities, while a 12-character password with lowercase and uppercase letters, numbers, and symbols offers around 19 x 1,021 possibilities.

To put it into perspective, even if a computer could crack the six-character password in one second, it would take more than two million years to crack the 12-character password.

Essential Cybersecurity Tips

Here are some crucial tips to enhance your cybersecurity:

1. Implement multi-factor authentication (MFA):
   - According to Microsoft, using MFA reduces the likelihood of a compromised account by more than 99.9 percent.
2. Use a "passphrase":
   - Create a long yet memorable phrase that is easy to type but hard to guess.
   - For example, transform "I Love Pizza with Onions!" into "IL0v3Pizz@with0ni0ns!"
   - This 21-character passphrase is both difficult to crack and easy to remember.
3. Avoid reusing passwords:
   - Utilize a different strong password for each account to prevent credential-stuffing attacks.
4. Longer is better:
   - Ensure each password is unique and not easily guessable.
5. Don't write passwords down:
   - Avoid storing passwords in insecure locations, such as sticky notes or computer files.
6. Be cautious of phishing emails and sites:
   - Stay vigilant against social engineering attempts to steal personal information.
7. Regularly monitor your accounts:
   - Routinely check your online accounts for any signs of unauthorized access.
8. Sign up for data breach notifications:
   - Stay informed about potential breaches by subscribing to services like Have I Been Pwned?.
9. Change passwords after a data breach:
   - If you discover a data breach, immediately change your password and monitor for any suspicious activity.

brightflow
TECHNOLOGIES

The Importance of Password Managers

Handling numerous intricate passwords can feel like an uphill battle for many of us. This is precisely where the assistance of password manager apps becomes invaluable.

These apps not only take on the responsibility of creating and recalling complex credentials but also ensure that the login process is smooth and hassle-free.

Whether you opt for 1Password, LastPass, Bitwarden, or Dashlane, the choice is yours – import logins from your browser or start anew. These apps go the extra mile by generating robust passwords for new sites and seamlessly auto-filling them as you navigate the web.

One of the key advantages of embracing password managers is their ability to thwart "credential stuffing" attacks. Picture this: a cybercriminal gains access to your compromised password on a platform like Facebook and then attempts to infiltrate other popular services you use, such as Spotify, Amazon, or Netflix. Here's where password managers step in as your digital guardians.

Moreover, these managers also provide an added layer of defense against phishing attacks, shielding you from scammers attempting to trick you into revealing your valuable credentials. Remember, your security matters and a reliable password manager can make all the difference.

Why We Recommend Password Managers

We completely understand the reservations that might come up when considering entrusting all your passwords to a single app. However, it's crucial to note that the chances of a password manager being breached are exceptionally low.

These apps prioritize the security of your logins by encrypting them, ensuring that access is granted only with your master password. Importantly, passwords are never stored in plain text on your device or the password manager's servers, rendering them off-limits to hackers.

In the rare event of a breach, as witnessed in the LastPass incident of 2022, our recommendation is straightforward: change your master password and generate new passwords for all your accounts. This precautionary step ensures an additional layer of protection.

When you opt for a robust password manager, you are actively enhancing your cybersecurity hygiene. It's worth noting that this perspective is widely shared by cybersecurity experts who recognize the value of these tools in safeguarding your digital assets. Your security is of utmost importance, and a trustworthy password manager is a key player in fortifying your online defenses.

Are Your Passwords Strong Enough?

The significance of securing passwords and fortifying their strength cannot be overstated, whether you're an individual or a business entity. Staying proactive in the face of cybersecurity challenges may appear daunting, but it is an essential responsibility.

If you're eager to learn more about the latest cybersecurity trends or elevate the security measures of your business, let’s chat.

Your security matters, and we're here to empower you with the tools and knowledge you need.

brightflow
TECHNOLOGIES

Is Your Company Protected?

Managing passwords and making sure they're at their strongest is a priority for all businesses and enterprises. Staying on top of cybersecurity concerns, however, can be a daunting task.

If you want to learn more about the latest cybersecurity trends or want to button up your business, let's chat.

brightflow
TECHNOLOGIES

REFERENCES

https://cloudnine.com/ediscoverydaily/electronic-discovery/80-percent-hacking-related-breaches-related-password-issues-cybersecurity-trends/

https://www.comparitech.com/blog/information-security/password-statistics/

https://www.intrust-it.com/lastpass-incident/

https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

https://www.theguardian.com/technology/2022/mar/19/not-using-password-manager-why-you-should-online-security

https://haveibeenpwned.com/

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-10000.txt

https://www.scientificamerican.com/article/the-mathematics-of-hacking-passwords/

(704) 585-1010

brightflow.net

4475 Morris Park Drive , Suite B
Mint Hill, NC 28227