Password Security.

Gone are the days when you could use a simple 'easy to remember' password on every site you needed to use a password on to access it. These days we might find that the average person requires log in details for over 100 sites.

The number is gradually increasing as our lives become more and more dependent on websites for services from mundane things to the important things like healtcare and banking.

Therefore password security is just as important as having your annual health check.

Here are some tips on how to make sure you aren't breaking any fundemental password rules.

1. Make your passwords long
2. Avoid common phrases (in any language)
3. Do not use personal information
4. Use a mix of characters and UPPER and lower case letters, numbers and symbols
5. **NEVER** reuse passwords, even on 'low priority sites'
6. Store passwords in a secure password manager
7. Only change a password when you need to or if there has been a data leak
8. Use 2-factor authentication
9. Only share passwords securely
10. Be careful clicking on links in emails/text messages

1. **Make your passwords long**: Increasing password length is among the most important password security tips. The logic behind longer passwords is simple each time you add an extra character, you increase the number of possible combinations, along with the time it would take an attacker to decipher the password. Just going from 8 to 12 characters makes it nearly impossible to guess a password based on computer-generated combinations.

2. **Avoid common phrases**: Dictionary words like *password, dragon*, *monkey* and *princess* are among those commonly used as a password (or part of one). Not surprisingly, these simple words, along with basic patterns like *abcd1234,* are also easy for others to guess. Numerical passwords like *123456789* are even less secure since there are only ten available characters.

3. **Do not use personal information:** Most of us are guilty of this occasionally. After all, it's much easier to remember your parakeet's name than some random combination of numbers and letters. Addresses and birthdays are other examples of personal information that people convert into passwords to make them easier to remember. Since this identifying information can often be found on the web, leave it out of your passwords.

4. **Use a mix of characters:** Using a variety of symbols in your password, including uppercase letters, lowercase letters, numbers, and special characters, is another good way to strengthen password security. Since there are no set rules for arranging the symbols, try inserting special characters and uppercase letters into the *middle* of the password, not just the beginning or end. But while you may think it's clever to replace common letters with symbols, l!k3 th!$, be warned: cybercriminals are wise to this tactic, so it won't actually slow them down any more than regular words will. On some devices (iPhones etc) when logging in to a site for the first time it will offer a secure password... use it, it will then be saved.

5. **Never reuse passwords:** The volume of accounts and passwords we maintain can lead us to reuse passwords to make them easier to remember. Duplicate passwords weaken cybersecurity by exposing multiple accounts if even one password is compromised. Using a secure password manager will often alert you to duplicate and compromised passwords.

6. **Never store passwords in an unsafe place:** Passwords stored in desk drawers or written on sticky notes can easily be lost or fall into the wrong hands. Passwords stored electronically in spreadsheets, notes applications, or web browsers are also vulnerable since none of these methods typically use encryption to protect stored passwords. Use a secure password manager application such as 1Password, Dashlane, Password App built in to MacOS/iOS, NordPass, Keeper etc. Password managers will ensure that you no longer need to remember any passwords only the one to get in to the manager, and that can often be done with Face ID or Touch ID or similar.

7. **Only change your password when you need to:** Changing passwords too frequently can make them less secure. Changes might result in only minor changes to an existing password and if the previous password was compromised, then the hacker has a head start on what the new password might be.

8. **Use 2-factor authentication (2FA):** This uses a second credential, such as a randomly generated code sent through an app or by email/SMS to provide further verification that the user trying to log-in is the correct person. This is best set up with an application on your smart phone so only you will have access to it. Apps that offer this feature include Authy, Google Authenticator, Microsoft Authenticator, Duo Mobile as well as a lot of the password managers available now.
   Banks will insist on using 2FA to access your account these days. It doesn't replace your password, therefore your banking password and any other password you use on a site with 2FA should follow all the normal rules. It's also best to use 2FA on any social media sites you access.

9. **Only share passwords securely:** Try to avoid sharing any passwords with anyone if you can help it. If their security is impacted in some way then it compromises your security as well. It's best that they set up their own account rather than sharing yours when possible. Most of the password managers however offer a method of sharing data using encrypted and therefore secure methods. If you must use a messenger service to share important information choose one that has end to end encryption, and is not open such as email or an ordinary text message.

10. **Avoid clicking on links in emails:** It is very easy to get caught out by an email or text message that looks like it has come from a reliable source. Don't click on the links until you have checked if they are real or not. If have clicked on a link that compromised your security, make sure you change your password straight away do not wait. Keeping your email box empty of junk emails is a whole other topic for another day!

Passkeys: Passkeys are a new way to log in to apps and websites without using traditional passwords. Instead of remembering and typing in a password, you use a digital key that is unique to each account.

Here's how it works:

1. **Two Keys**: Your device creates two keys - a public key and a private key.
2. **Public Key**: The public key is stored by the app or website.
3. **Private Key**: The private key stays on your device and is used to unlock your account.

When you log in, your device uses the private key to prove your identity without ever sharing it. This makes it much harder for hackers to steal your login information

Passkeys are often used with biometric authentication like FaceID or fingerprint scans, making them both secure and convenient

Read more about Passkeys here. https://developers.google.com/identity/passkeys

Stay safe on line.
Steve Morton
August 2024