

SECURITY HINTS & TIPS



Keeping Your Passwords Squeaky Clean

Did you know that the average person uses the same three to seven passwords to log in to over 170 online accounts? In addition to being reused, these passwords are often weak and can be easily guessed by cybercriminals. If cybercriminals guess these passwords, they could access the majority of their victim's online accounts. Even worse, the victim may not know that their password has been compromised for several months or years. To keep your passwords squeaky clean and safe from cybercriminals, follow the tips below:

Create Strong Passwords

Creating strong passwords helps prevent cybercriminals from gaining access to your online accounts. Your passwords should be as long, complex, and random as possible. While many websites only require passwords to be eight characters long, we recommend making your password at least 12 characters long. You should also include a combination of lowercase and uppercase letters, numbers, and symbols in your password. To keep your accounts extra safe, you can use password phrases, or passphrases. However, when you create your password or passphrase, make sure that you don't use any personal information that a cybercriminal could guess.

Don't Reuse Passwords

Reusing passwords for your online accounts may be convenient, but it's also risky. If you reuse passwords, you could be at risk of having multiple accounts compromised at once. If a cybercriminal guesses your password, they could access multiple accounts instead of just one account. Cybercriminals can also sell passwords or make them available online. Creating a unique password for each online account reduces the risk if one of your passwords is compromised.

Use a Password Manager

You're probably wondering how you are supposed to remember long, complex passwords for all of your online accounts. The answer is a password manager. You can use password managers to securely store all of your passwords. Instead of having to remember passwords for every online account, you only have to remember one password for your password manager. In addition to storing your passwords, many password managers can also generate passwords for you based on specific criteria.

Use Multi-Factor Authentication

You can also use multi-factor authentication (MFA) to secure your online accounts, if available. MFA requires multiple forms of authentication, such as a password and a code from your smartphone or a USB smart key. By requiring you to use multiple forms of authentication, cybercriminals will have a harder time gaining access to your account, even if your password is compromised.

Nobody wants cybercriminals to guess their passwords. To keep your passwords squeaky clean and safe, remember to create strong passwords, avoid reusing passwords, and use a password manager or MFA, if possible.



The KnowBe4 Security Team
KnowBe4.com