6 Helpful Password Security Tips

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/helpful-password-security-tips/

By Vipin PG | Published September 15, 2022 | Updated March 8, 2026 | Format: Analysis | 4 min read

In brief

It’s no secret that passwords are a weak link in the security chain. Yet, we use our passwords everywhere and for everything.

It’s no secret that passwords are a weak link in the security chain. Yet, we use our passwords everywhere and for everything. For instance, passwords for banking, online shopping, email, or any type of website we visit.

Good passwords are important. However, there are way too many easily hackable password options like "qwerty." These bad passwords make it easy for someone to break into your account and get access to everything on it.

Did you know that it takes only 10 minutes for a hacker to figure out 6-character passwords? Additionally, 80% of hacked accounts are a result of password stealing. Considering these statistics and threats, you need to take some precautions. But first, you might wonder, how can your passwords be hacked?

There are endless ways cybercriminals can hack your password. Yet, the most common methods include phishing and password hacking software. In the second case, hackers use password hacking software to run an algorithm against a password until it cracks.

To not fall victim to these hackers, we have six helpful password security tips:

1. Use Longer Passwords with Diverse Characters

The more complex, unique, and long a password is, the less likely it is to be guessed. If you make it hard for someone to think of your password, they’ll have a more challenging time stealing your account information.

Use numbers, punctuation, special characters, and both upper- and lowercase letters in your writing. In a perfect scenario, you would use each character type. Try to avoid keyboard input, letter, and number patterns.

Mostly anyone knows that passwords such as 12345, ABCDE, and ASDFG shouldn’t be used. But a skilled hacker can detect when letters are replaced with identical numbers or special characters. Therefore, changing the letter "o" to "0," I to "1," or "a" to "@" is pretty useless. Instead of such replacements, try to use a special character, like "$," for instance.

You should check out the list of the most commonly used passwords. Make sure you never use these, or you will compromise your digital security.

2. Don’t Use The Same Password On Multiple Accounts

If you use the same password on multiple accounts, someone could guess your password and break into all the sites you logged in to at once. That’s a nightmare scenario because they can easily access your personal information, like credit cards and bank accounts.

Every account needs a different password. You shouldn’t, for instance, use your Twitter password for mobile banking or your Facebook password for your workplace.

3. Change Your Password Frequently

Changing your password is one of the most important things you can do to protect yourself and your digital life. Over time, a hacker might attempt to log into your account more than once. Frequent changing of your password lowers the likelihood that they will gain access. Try changing your password at least once every six months.

4. Don’t Use Personal Information As A Password

Don’t use personal information such as your name, home address, or phone number as a password. People use these kinds of passwords as it is easy for them to remember. This is a big mistake because it makes it easy for hackers to get your public information and then use it to crack your password.

5. Use Multifactor Authentication

MFA, or multi-factor authentication, has become necessary to safeguard your online accounts. For example, MFA asks you to enter a multi-digit code from an app like Facebook or Google Authenticator to log in to your account.

Using MFA has a significant impact on digital security. MFA, according to Microsoft, can block 99.9% of cyberattacks on your accounts. But unfortunately, it’s a common business practice; some online banking services provide MFA as an option, so you have to turn that function on.

MFA is also becoming more user-friendly. For example, most people are familiar with the version in which a code is texted to you.

6. Start Using Password Managers

If you have a lot of online accounts, it can be hard to track them all. A password manager can then help you create strong, unique passwords that will be stored in one secure place.

They also help protect your passwords from being hacked by keeping them on their internal servers instead of on your computer. Therefore, even if someone hacks into your computer and steals all of your personal information (such as names and addresses), they won’t be able to access those passwords.

Just use a trusted password manager with end-to-end encryption, like NordPass. That’s the only way your security can be guaranteed. You may download an app for your phone to check it out.

Conclusion

Passwords play a significant role in our digital security. However, using complex and unique passwords for each online account doesn’t have to be complicated. Following these six easy tips will significantly enhance your security and protect you from cybercriminals.

References

1. phishing.org - what-is-phishing - https://www.phishing.org/what-is-phishing

2. play.google.com - store / apps - https://play.google.com/store/apps/details?id=com.nordpass.android.app.password.manager