

Student Knowledge Base



SOUTH ALLEGHENY
SCHOOL DISTRICT

STKB057 Safe Password Recommendations

The security of your bank account, Netflix account, and email inbox depends on how well you safeguard your passwords.

Strong passwords are of course key to your security. The challenge is to create strong passwords you can actually remember, without stumbling into the bad habits that can harm you -- like reusing the same password for multiple accounts. But how many passwords can you actually remember? You could easily have 85 passwords for all your accounts, from banking to streaming to social media, according to LogMeIn, which makes the LastPass password manager.

Weak passwords, or overusing the same password, can have serious consequences if your data is compromised -- even if that password is strong. For example, companies reported 5,183 data breaches in 2019 that exposed personal information like login credentials and home addresses that someone could use to defraud you or steal your identity. And since 2017, hackers published 555 million stolen passwords on the dark web that criminals can use to crack into your accounts.

Password security may not completely prevent your data from being exposed, but these best practices can help minimize your risk if it is. Here's how to create and manage the best passwords, how to find out if they do get stolen, and one essential tip to make your accounts even more secure.

Avoid common words and character combinations in your password

The goal is to create a password that someone else won't know or be able to easily guess. Stay away from common words like "password," phrases like "mypassword" and predictable character sequences like "qwerty" or "thequickbrownfox."

Also avoid using your name, nickname, the name of your pet, your birthday or anniversary, your street name or anything associated with you that someone could find out from social media, or from a heartfelt talk with a stranger on an airplane or at the bar.

Longer passwords are better: 8 characters is a starting point

8 characters are a great place to start when creating a strong password, but longer logins are better. The Electronic Frontier Foundation and security expert Brian Kerbs, among many others, advise

using a passphrase made up of three or four random words for added security. A longer passphrase composed of unconnected words can be difficult to remember, however, which is why you should consider using a password manager.

Don't recycle your passwords

It's worth repeating that reusing passwords across different accounts is a terrible idea. If someone uncovers your reused password for one account, they have the key to every other account you use that password for.

The same goes for modifying a root password that changes with the addition of a prefix or suffix. For example, PasswordOne, PasswordTwo (these are both bad for multiple reasons).

By picking a unique password for each account, hackers that crack into one account can't use it to get access to all the rest.

Avoid using passwords known to be stolen

Hackers can effortlessly use previously stolen or otherwise exposed passwords in automated login attempts called credential stuffing to break into an account. If you want to check if a password you're considering using has already been exposed in a hack, go to [Have I Been Pwned](#) and enter the password.

No need to periodically reset your password

For years, changing your passwords every 60 or 90 days was a long-accepted practice, because, the thinking went, that was how long it took to crack a password.

But Microsoft now recommends that unless you suspect your passwords have been exposed, you don't need to periodically change them. The reason? Many of us, by being forced to change our passwords every few months, would fall into bad habits of creating easy-to-remember passwords or writing them on sticky notes and putting them on our monitors.

Use two-factor authentication (2FA) ... but try to avoid text message codes

If thieves do steal your password, you can still keep them from gaining access to your account with two-factor authentication (also called two-step verification or 2FA), a security safeguard that requires you enter a second piece of information that only you have (usually a one-time code) before the app or service logs you in.

This way, even if a hacker does uncover your passwords, without your trusted device (like your phone) and the verification code that confirms it's really you, they won't be able to access your account.

While it's common and convenient to receive these codes in a text message to your mobile phone or in a call to your landline phone, it's simple enough for a hacker to steal your phone number through SIM swap fraud and then intercept your verification code.

A much safer way to receive verification codes is for you to generate and fetch them yourself using an authentication app like Authy, Google Authenticator or Microsoft Authenticator. And once you're set up, you can choose to register your device or browser so you don't need to keep verifying it each time you sign in.

When it comes to password security, being proactive is your best protection. That includes knowing if your email and passwords are on the dark web. And if you discover your data has been exposed, we guide you through what to do if hackers have gained access to your banking and credit-card accounts.

Use a password manager to keep track of your passwords

Strong passwords are longer than eight characters, are hard to guess and contain a variety of characters, numbers and special symbols. The best ones can be difficult to remember, especially if you're using a distinct login for every site (which is recommended). This is where password managers come in.

A trusted password manager such as 1Password or LastPass can create and store strong, lengthy passwords for you. They work across your desktop and phone.

The tiny caveat is that you'll still have to memorize a single master password that unlocks all your other passwords. So make that one as strong as it can be (and see below for more specific tips on that).

Browsers like Google's Chrome and Mozilla's Firefox also come with password managers, but our sister site TechRepublic has concerns about how browsers secure the passwords they store and recommends using a dedicated app instead.

Password managers with their single master passwords are, of course, obvious targets for hackers. And password managers aren't perfect. LastPass fixed a flaw last September that could have exposed a customer's credentials. To its credit, the company was transparent about the potential exploit and the steps it would take in the event of a hack.

**Contact the Help Desk with any questions.
tech@st.southallegheny.org**