Password Protection

How to Create a Strong Password

Choosing a **strong password** is the first step in password protection. If a person were trying to guess your password, they might try ten or so passwords a minute if they're fast. A computer can guess much, much faster. So how many permutations does it take to get your password?

Here are three key factors:

- **Length.** Each character increases the complexity exponentially. Therefore, passwords typically have a minimum requirement of 8 characters.

- **Character sets.** Each character set has a certain number of permutations. There are 26 lowercase letters, but only 10 digits (0-9), so you can see how "summer" is more secure than "536871" from the perspective of a machine running through different combinations of characters.

- **Common words.** A computer can run a "dictionary attack" against a password very quickly, testing for all real words, of which there are relatively few, compared to the huge number of character permutations possible. Suddenly "summer" isn't that great of a password after all.

Your password should be a combination of at **least both upper** and **lowercase letters** and a **number**. You should also include a **special character** to increase complexity, but make sure the character is supported by the mechanism you are using, as some are not.

You can find any number of password generators online, which can generate extremely complex passwords. Keep in mind that having separate passwords for every account can be too much to ask, with 18 character randomly generated passwords (see password managers section).

Change Your Password

Some service providers require and prompt regular password changes, while others do not. It's always a wise idea to change your password regularly – just in case! This is an important strategy to minimize risk and protect your private, personal information. We know, this may seem annoying but it's nothing compared to dealing with a compromised account, credit card fraud, or identify theft! Set a reminder on your phone/calendar.

Shhh…

Never Share Your Password

Never share your password with anyone!

Ideally, your password should only be in your head. If you must write it down, keep the password in a locked and secured location.

Different Site? Different Passwords

Many people will also use the same password for all their sites, which again increases the risk of compromise and exploitation. If a hacker cracks the code for one area of your life, they may have cracked them all! Even something as simple as adding a suffix or prefix to your passwords to differentiate them, for instance 'fb' for Facebook (i.e., **fb**TM4256lpg7) will prevent most cross-site compromises.

Don't Reuse Passwords

Most people choose to alternate between passwords, but this doesn't have the same effect as changing them to something new each time. Once a password is compromised, it can be exploited at any point in time – even years later! Choosing to reuse passwords increases your vulnerability and risk at being compromised.

Secure Your Reset Options

This approach protects you from people, rather than computers, who are trying to hack into your account. It's important to be thoughtful with your security questions and don't choose ones for which the answers are publicly available. Many people's accounts are hacked by people they know in real life. If you have an email account where password resets will be sent, be sure you are the only one who has access to it and that it too has a strong password to protect it.

Passwords Manager

Think carefully before you choose to use a password manager to store your passwords. The major browsers all have password storage systems, while the phone applications and cloud-based options work from any computer with internet access. The positive aspect of this is you don't have to remember all your passwords. The negative and even more concerning aspect is, that now your browser automatically logs you in so if your PC or laptop is stolen – someone else has instant access to ALL your accounts!

Don't Leave Windows on Your PC Open

If you are using a computer accessible by others, especially the public be sure to close the entire browser process when you are done. If you don't shut down the browser entirely, you may leave your session cookies available for the next person – which means they may have easy access to your information.

2-Factor Verification

Probably one of the most important mechanisms available, 2FA, as its name implies, prevents the compromise of a single authentication factor (the password) from compromising the account. The mechanism typically works by requesting the traditional login information, then sending a confirmation to a device, usually a smartphone, such as a text, phone call, or in-app security verification screen. Ideally, only the authorized person would have the smartphone and could then accept or reject the authentication requests as necessary. This is becoming more common!