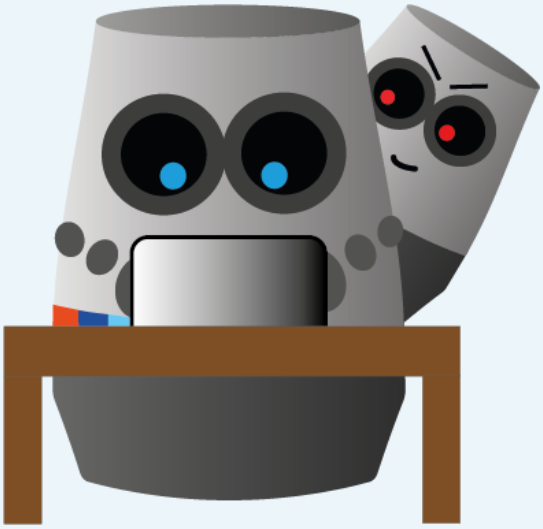


Password Management & Security

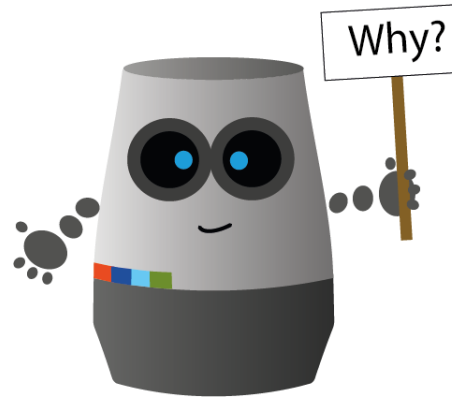
A guide to creating and managing secure passwords

SWGfL
Safe, Secure, Online

Contents

Why password security is important

In a digital world, your passwords are like your keys. If someone finds one of your passwords, they effectively have a copy of your key.



Just like a key, if a password is strong and kept secure, it shouldn't really ever need to be changed. And just as you don't use the same key for your house and car, you shouldn't use the same password for different websites.

Multiple people should not use the same username and password to access a system. If there is an issue, it makes it difficult to determine who performed what actions.

In the event of a breach, being able to trace it to an individual account speeds up the investigation and can limit the damage to whatever access the breached account had.

How passwords are secured

In well-designed systems, your password will be encrypted with a one-way hashing algorithm when it is stored.

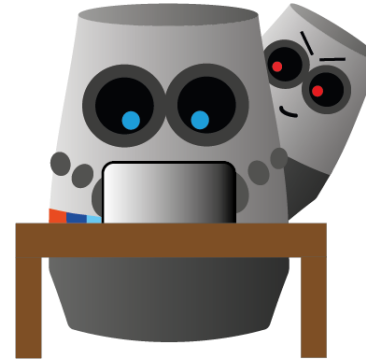
Hashing works by turning your password into a string of letters and numbers that cannot be turned back to the password mathematically.

When you log in, the same hashing is applied to the password you typed and the two hashes are compared.

It's quite quick to turn your password into a hash, so most systems use an algorithm that then hashes it again, and again, and again. This makes generating one hash still relatively quick, but it is much slower to attack a password hash with brute force (Trying every combination).

How passwords are stolen

Attackers use a range of methods to attempt to steal passwords, including:



- Shoulder-surfing: someone watching you closely as you log in and attempting to remember the keys you used
- Key-logging: a device (or piece of software) installed by an attacker to intercept the passwords you type in
- Social engineering: an attacker trying to convince you to reveal your password to them
- Guessing: an attacker simply using information they know about you to guess your password
- Physical searching: an attacker searching the area around your device for insecurely stored passwords (e.g. written down)
- Network searching: an attacker scanning the ICT systems for insecurely stored password information
- Intercepting: an attacker 'breaking in' to information transmitted over a network (including the internet) and looking for password details
- Brute force: an attacker using a system to try millions of different passwords automatically to attempt to find the correct one

How long does it take to crack?

When a system is compromised, the hacker may gain access to your user name and other associated information, but if the password is hashed, the hacker wouldn't immediately be able to use it. To do so, hackers may then use a brute force attack to crack the password.

This is where having a long password helps: password length increases the entropy (number of combinations) and makes calculating each combination take longer.

Using upper/lower/numbers/symbols, each character may have 256+ possible combinations. A hacker may speed up cracking your password in several ways, e.g. by assuming you only used lower case letters, which would make only 26 possible combinations per character.

The time it takes to crack a password depends on a lot of factors, such as entropy and computer speed, but as a guide:

Length	Time to crack
7 characters	<1 second
8 characters	~5 hours
9 characters	~5 days
10 characters	~4 months
11 characters	~10 years
12 characters	~200 years

Password formats and policies

Cracking passwords can take less time if the hacker knows the password format. This is why enforcing complexity in a password policy (e.g. 'must contain an upper-case letter') can be counter-productive. The hacker could assume the upper-case letter will always be the first letter, thus lowering the number of possible combinations.

Password policies that require users to frequently change passwords may also increase risk, as users will be more likely to write passwords down or store them insecurely but to hand, to avoid being unable to access systems.

Passwords should be easy for users to change, but you should only encourage users to change good passwords if they suspect they have been compromised.

Creating good (secure) passwords

A secure password is one that is easy to recall, but hard to guess or crack.

Bear in mind that for every character added to the password, the number of combinations is exponentially increased – so in a strong password, length is the only thing that really matters.

If you struggle to remember 'complex' passwords, use fewer character types, but make the words longer and part of a pattern that only you know:

Pattern	Password	Recall	Guess	Crack
Name of dog	MrPoochy	Easy	Easy	Easy
All char types	$rjUa^*j	Hard	Hard	Easy
All char types	7\[o|;r@Bm"!]jS	Hard	Hard	Hard
Song lyrics	i wanna dance with somebody	Easy	Easy	Hard
Objects in a photo	tree ocean motorbike helmet	Easy	Hard	Hard
4 random words	town simplest each solve	Easy	Hard	Hard

How to manage your passwords

The trick to keeping a password secure is to remember it and not write it down anywhere (unless you keep it in a secure location).

Remembering passwords can be difficult, especially when you have accounts on many different systems. It can be tempting to use the same one on all of them.

If you struggle to remember all your passwords but want your accounts to be secure, consider using a password manager with a long, easy-to-remember master password.

A password manager (or password vault) is a secure website allowing you to store the log in information for all the other websites you access.

You can then generate long, random passwords for each system you access, store them in the password manager, and you only need to remember the one password for the password manager.

How to protect your password

Passwords can be compromised in a number of ways, many of which can be mitigated:

Method	Solution
Telling someone	Never tell anyone your password. Ever
Storing in an insecure place	Use a password manager. Or use a secure place to store written passwords
Making it too easy to guess	Use secure passwords, and don't include personal information
Shoulder surfing	Make sure no one can see you enter your password
Stolen by a key-logger	Install anti-virus software and keep your computer up to date
Intercepted over the network	Only enter passwords over an encrypted connection (https)
Password stolen from another system	Use different passwords for each system you access

In a correctly designed system, you should never need to reveal a password to anyone.

Managing passwords for others

From time to time you may be required to set up access to a system for another person.

A well-designed system should implement a zero-knowledge policy – only allowing the system and the user to have access to the password. But sometimes this may not be possible.

If you have to give a user their password, make sure to generate a long and hard-to-remember password. This will prevent you from recalling it, and encourage the user to change their password immediately.

Never give anyone else access to your account, even if just temporarily. You can always create a temporary account for them with limited access, and delete the account after use

Password security checklist

Creating Passwords

- ☐ Create easy to remember passwords that are hard to guess/crack
- ☐ Use passwords that have no association with you
- ☐ Use long passwords (14 characters+)
- ☐ Use different passwords for each account

Protecting Passwords

- ☐ Remember secure passwords, don't write them down
- ☐ Never tell anyone your password or give access to your account
- ☐ Keep software up to date
- ☐ Beware of shoulder surfers

Managing Passwords

- ☐ Use a password manager
- ☐ Reset passwords with a long random string when your password manager is not to hand

Password Policy

- ☐ Only enforce length as a requirement
- ☐ Implement zero-knowledge by enabling users to create their own passwords
- ☐ Where zero-knowledge is not possible, generate long random passwords and recommend password change on first login