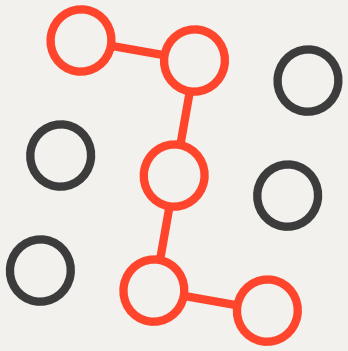
kyndryl

What makes a good password

Password lists are freely available on the internet. They are often shared, sold to other cyber criminals, and used to gain entry to multiple websites.[1]

A strong password consists of:

- At least 15 characters
- Small and capital letters
- Numbers
- Special characters
- Unique phrase



Strong passwords can take millions of years to hack.
Weak passwords take seconds.

Strong password best practice advice:

- Don't use the same password across accounts.
- Don't share them with colleagues or family.
- Don't save them in the browser.
- Don't use personal birthdays, pet names, etc.[2]

Why should you use 1Password? It is an electronic "Password Vault" which makes it very hard for the hackers to break through.

- Suggests complex, hard to guess passwords.
- Helps you securely store and sync complicated passwords.

- Notifies you about password breaches and other security problems.
- Allows to use your fingerprint without entering a password.

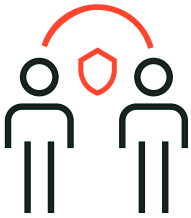
- Allows you to remember and use only one password to login to all your accounts and assigned passwords stored in the vault.
- Allows you to share 1Password with your family members – it is FREE.

Examples:

You have too many passwords to remember. You decide to store your passwords in your browser, not realizing the significant risk.

When your site/account is compromised, the first place the attacker looks is in your browser storage and this will provide the attacker the opportunity to steal your personal or professional identity.

You're using your birthplace or your mom's maiden name as password, then cracking your passwords is just a matter of time.[3]

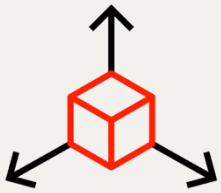


These are easy passwords to find on social media. Never use any personal information (name, birthday, username, email address) in a password. Using passphrase such as "Pattern2baseball#4mYmiemale" is more secure.

Your friends are telling you they have received strange emails from your email account, and some have inappropriate content and photos.

This usually means your email password has been hacked and if that same password was used on other accounts, then they are also at risk. You need to change your email password immediately and make it a strong secure password for all your accounts.

You receive a text from your bank asking you to confirm a large sum payment with instructions to text back to confirm yes or no.



You panic because you didn't make the purchase; therefore, you text "no". The next instruction is to provide the one-time-password sent to you in a different text. Don't fall prey to this. Never respond to these types of texts. Never provide one-time-passwords to anyone. Contact your bank directly to resolve any concerns.

For more information, explore more references and visit the following pages:

1. This Hacking Horror Story Is a Warning to Take Online Security More Seriously. https://www.rd.com/article/hacking-horror-story/
2. What is Password Hacking? https://www.veracode.com/security/password-hacking
3. Mark Zuckerberg's Terrible Password Revealed in Hack. https://www.vanityfair.com/news/2016/06/mark-zuckerberg-terrible-password-revealed-in-hack