FIELD EFFECT™

5 secrets for stronger passwords

Passwords became a security problem instead of a solution. Weak or previously compromised credentials can offer easy entry for attackers.

Discover five secrets to a stronger password, plus bonus tips to keep your accounts extra secure.

01

Add complexity to your passwords.

Strive to use longer passwords that include upper and lowercase letters, numbers, and special symbols.

During a brute-force password attack, sophisticated cyber criminals may use software to generate potential combinations. The more elaborate your password is, the longer this process takes, and the more likely the attacker gives up or gets caught.

Consider this: a four-character password of only lowercase letters has 456,976 possible combinations — a manageable number for attackers with the right technology. Double the length to eight characters, and there are now 209 billion possibilities.

BONUS TIP:
Avoid typical replacement characters, such as "@" in place of "a."

02

Use passphrases instead of traditional passwords.

Passphrases — strings of words that make sense to you, such as 1BlackCabinetSpiderPlant! — are naturally longer and therefore more resilient to compromise. Many cyber security experts recommend this approach, including the National Institute of Standards and Technology (NIST)[1] and the Canadian Centre for Cyber Security (CCCS).[2]

Plus, passphrases are typically much easier to remember than random combinations of combinations of letters, numbers, and symbols.

03

Avoid including any personal information.

Studies show that too many account holders still use significant dates, family names, pet names, and other personal information in their passwords.[3] This is a problem because cyber criminals often research potential victims, browsing their social media accounts where these personal details may be available. It's much easier to crack a password that contains public information.

BONUS TIP:
Avoid choosing security questions if the answer can be found online.

04

Use unique passwords for every account.

One really critical cyber security rule is to never reuse passwords. If a large-scale breach exposed your credentials for one portal or application, every account that uses the same password would also be at risk.

But it's not easy to memorize multiple unique passwords, which may explain why only 35% of account holders follow this best practice.[4]

05

Autogenerate complex credentials with a password manager.

A password manager tool allows you to create, store, and retrieve strong passwords for your accounts. With the ability to autogenerate complex strings of letters, numbers, and symbols, you can use unique passwords without having to remember them all.

When evaluating password manager tools, look for one with:

- A positive reputation among clients
- Reasonable pricing
- Strong cyber security standards
- Support for your platforms (iOS, Linux, etc.)

Find these tips helpful?

Share this list with colleagues or others who may want to boost their password security. If you have any questions about these tips or cyber security in general, our experts are here to help.

Sources

1 https://pages.nist.gov/800-63-3/sp800-63b.html
2 https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032
3 https://www.ncsc.gov.uk/news/national-pet-day-password-advice
4 https://services.google.com/fh/files/blogs/google_security_infographic.pdf

fieldeffect.com
letschat@fieldeffect.com

Canada and the US
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT