A strong password is critical for keeping your private information secure, whereas a weak password invites criminals to steal your data. Below, we’ve listed some of the best and worst password practices.

**Don’t**

**Use predictable passphrases, like 123456**

Commonly used words and numbers are more easily cracked. Instead, combine random uppercase and lowercase letters, numbers, and symbols.

Don’t

**Use a social login**

Social engineers can identify your common passwords based on information shared on your profile. With access to your social profile, they have access to everything.

Don’t

“**Remember**” your password in a web browser

If you do, anyone with remote or physical access to your computer can use your passwords. Instead, use a secure password management app to keep track of your passwords.

**Do**

**Lengthen your password**

Every character you add to your password makes it exponentially more difficult to crack.¹

![Graph showing the increase in difficulty with longer passwords.]

**Do**

**Use a unique password for each account**

Otherwise, every account using the same password is vulnerable if one is breached.

**Average User’s Number of Accounts**

26

**Average User’s Number of Passwords**

5

**Do**

**Change your password periodically**

It can take months to learn about a data breach, so stay ahead of the news. It can take up to 205 days before the average data breach is detected.

**Remember:**

Never give out your password when it is solicited via email. It’s probably a phishing scam. If you believe you’ve been targeted by a spear phisher, play it safe and report it immediately.

---

¹ Source: [https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf](https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf)