

Strong Passwords & Passphrases

Weak passwords are one of the easiest ways for hackers to break into accounts. A single compromised password can put both personal and company data at risk. Treating passwords like the keys to your digital life is essential.



How Attacks Happen

Stolen Databases

When websites are breached, stolen credentials often end up for sale on the dark web. If you reuse the same password across accounts, one breach can compromise many logins at once.

Tip: *Never reuse passwords across multiple sites or services.*

Compromised Accounts

If a password is guessed, stolen, or leaked, attackers may already have access before you notice. The longer you wait to act, the more damage they can do.

Tip: *Change your password immediately if you suspect compromise.*

Password Cracking

Attackers use automated tools to guess millions of password combinations in seconds. Short or simple passwords are often cracked instantly.

Tip: *Create long passphrases made up of random words, such as "TreeHorseSunshine," which are harder for machines to guess but easier to remember.*

Forgotten Logins

Managing dozens of unique passwords is difficult, which leads many people to write them down or choose weak ones. This creates new risks if those notes or files are exposed.

Tip: *Use a trusted password manager to generate and securely store strong, unique passwords.*

