A HACKER'S SECURITY GUIDE // INFOGRAPHIC 02/08

THE PROTECTION LADDER: FROM PASSWORDS TO PASSKEYS

Every level you climb dramatically reduces the odds of having an account stolen.
Find out which step you're standing on today.

>> LEVEL UP

LEVEL 0 — DANGER ZONE

Weak or reused password

Built from personal info, easy to guess, or shared across services: if one is compromised, they all fall.

LEVEL 1

Strong password

Uppercase, lowercase, numbers, and special characters. Use a mnemonic rule: for example, the first letters of a phrase.

LEVEL 2

Unique per service + password manager

A different password for every system. With many accounts, a password manager remembers them for you.

LEVEL 3

Multi-factor authentication (MFA)

A second factor on top of your password: even if it's stolen, it's not enough to get in.

LEVEL 4 — THE GOAL

Passkeys

Passwordless access tied to your device: there's nothing to steal or guess through phishing.

>> RULES THAT APPLY AT EVERY LEVEL

→ Don't share your passwords

If an emergency forced you to share one, change it immediately afterward.

→ Hard security questions

If anyone can answer them using your public info, they're an open door.

→ Don't write them on paper or in files

No notebooks, no phone notes. If there's no other way, keep the paper somewhere very secure.

→ Change them fast after strange activity

If you spot odd activity on an account, change the password right away. And refresh them from time to time without waiting for the system to force you.

WATCH OUT

Make sure no one is watching while you type your password: prying eyes steal passwords too.