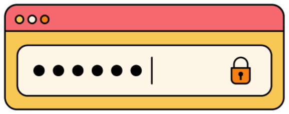
17 FACTS ABOUT PASSWORD

********* SECURITY

PENETRA
CYBERSECURITY

www.penetracyber.com



Passwords like "123456" and "password" are still among the most commonly used, making them extremely vulnerable to hacking.

Over 80% of data breaches are due to weak or stolen passwords.

Password managers can be a single point of failure if their master password is compromised.

Social engineering tactics, such as pretending to be technical support, can manipulate users into divulging their passwords.

Dictionary attacks use common words or phrases to crack passwords more efficiently.

Brute force attacks can guess passwords by trying every possible combination, exploiting weak or predictable patterns.

Shoulder surfing, where attackers observe users typing their passwords, remains a low-tech but effective method of password theft.

Biometric authentication, like fingerprints or facial recognition, can also be vulnerable to hacking, as seen in various security breaches.

Even complex passwords are vulnerable if stored improperly, such as in plaintext or weakly encrypted formats.

Approximately 30% of users reuse passwords across multiple accounts, amplifying the risk if one gets compromised.

Weak security questions used for password recovery can be easily guessed or researched, compromising the account's security.

Rogue Wi-Fi networks can capture passwords transmitted over unsecured connections, such as public Wi-Fi hotspots.

It takes hackers less than a second to crack a weak password using automated tools.

Keyloggers silently record keystrokes, including passwords, without the user's knowledge.

Password spraying attacks attempt to access multiple accounts using commonly used passwords, increasing the chance of success.

Phishing attacks trick users into revealing their passwords by mimicking legitimate websites or emails.

Password expiration policies can lead to users choosing weaker passwords or writing them down to remember, reducing security.