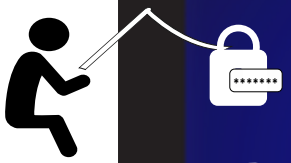
22
The average number of online passwords that each UK citizen has.

How passwords are discovered...

Attackers use a variety of password discovery techniques, including the use of powerful tools that are freely available on the Internet.



Social Engineering

Attackers can use social engineering skills to coerce users into revealing their passwords.

Shoulder Surfing

Observing someone typing in their password.

Manual Guessing

Attackers use personal information 'cribs' (such as name, date of birth, etc.) to guess common passwords.

Key Logging

An installed keylogger intercepts passwords when they are typed into a device.

4
Average no. of websites that users access using the same password.

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Stealing Passwords

Attackers can steal passwords that have been stored insecurely. This can include handwritten passwords hidden close to a device.

Searching

Searching IT infrastructure for electronically stored password information.

...and how to improve your system security.

The following advice will reduce the workload on your users, making your system more secure as a result.

Help users generate appropriate passwords

Put technical defences in place so that simpler passwords can be used.

Steer users away from choosing predictable passwords, and prohibit the most common ones.

Encourage users to never re-use passwords between work and home.

Train staff to help them avoid creating passwords that are easy to guess.

Be aware of the limitations of password strength meters.

Help users cope with 'password overload'

Only use passwords where they are really needed.

Use technical solutions to reduce the burden on users.

Allow users to securely record and store their passwords.

Only ask users to change their passwords on indication or suspicion of compromise.

Allow users to reset passwords easily, quickly and cheaply.

BLACKLIST THE MOST COMMON PASSWORD CHOICES.

MONITOR FAILED LOGIN ATTEMPTS, AND TRAIN USERS TO REPORT SUSPICIOUS ACTIVITY.

DON'T STORE PASSWORDS IN PLAIN TEXT FORMAT.

USE ACCOUNT LOCKOUT, THROTTLING OR MONITORING TO HELP PREVENT BRUTE FORCE ATTACKS.

PRIORITISE ADMINISTRATOR AND REMOTE USER ACCOUNTS.

CHANGE ALL DEFAULT VENDOR-SUPPLIED PASSWORDS BEFORE DEVICES OR SOFTWARE ARE DEPLOYED.

CESG

CPNI
Centre for the Protection of National Infrastructure