Password Security

Password Bingo!!

Write password down	Family members names as Password	Didn't change default Password
'123456' as your Password	'Your Date of Birth' as your Password	'Password' as your Password
Use the same password on multiple accounts	Added a number to the end of an old Password.	Shared your password with someone

Top Passwords

password
123456
sunshine
qwerty
Iloveyou
princess
admin
welcome
abc123
football

666666
123123
monkey
charlie
654321
!@#$%^&*
aa123456
donald
querty123
password1

stored password information.

can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.

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.

Searching

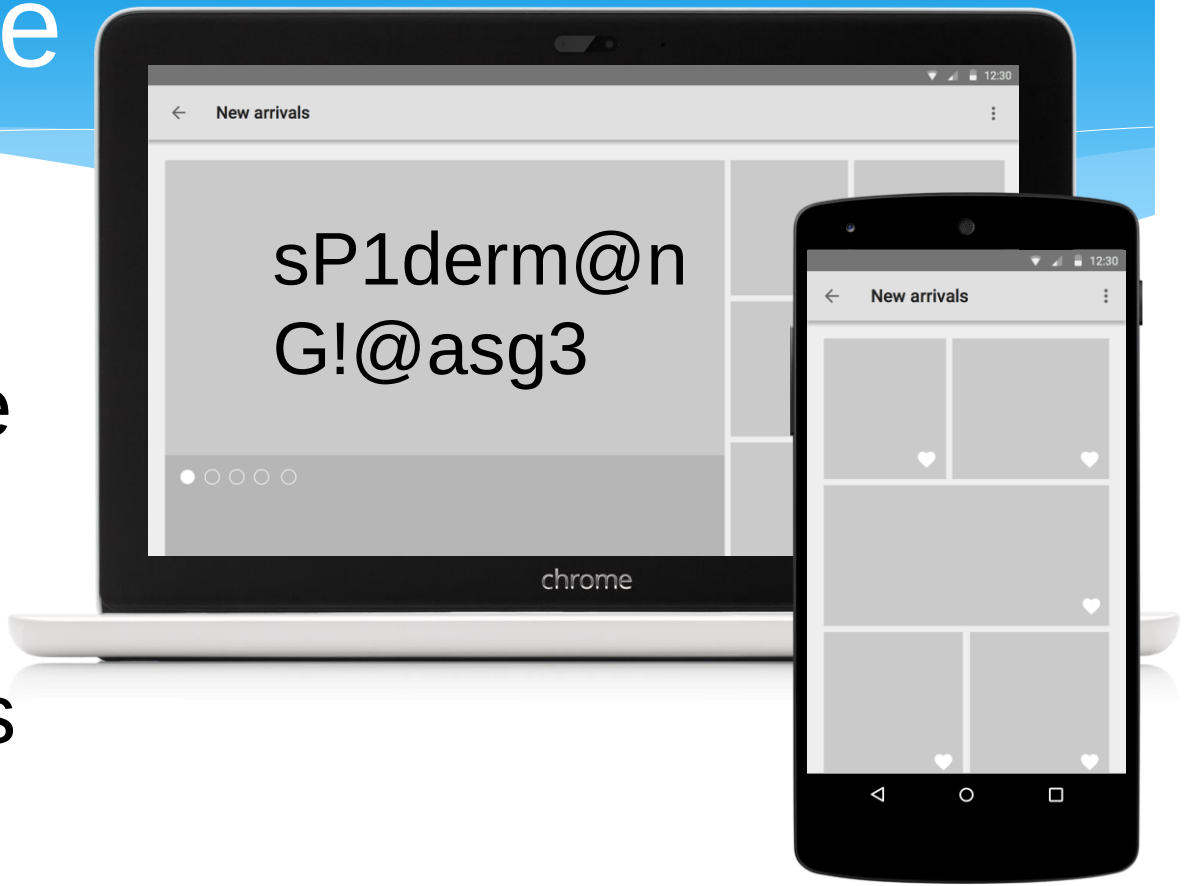
IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Brute Force

Automated guessing of large numbers of passwords until the correct one is found



G!@asg3

Think Three Random Words -

Passphrase Method

- embark jewel neuron
- Game of thrones
- my fluffy dog
- dusky mysterious cadet

Think Random!

Unique Password Everywhere

- Strong unique passphrase for every account
- Use a security tool to help you store and create passwords securely. - Password Manager

2FA

Two Factor Authentication

Next steps

- **3 word passphrase**
- **Use a password manager**
- **Turn on 2FA**

https://www.ncsc.gov.uk/

https://www.getsafeonline.org/

https://www.cyberaware.gov.uk/

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

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.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

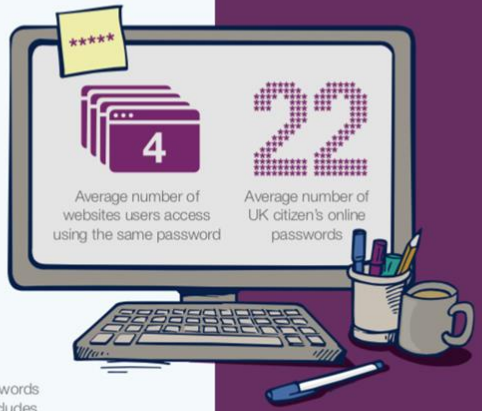
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

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 of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- 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.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

**** UPDATE

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc