Attacks on 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.

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

- **Shoulder Surfing**
  Observing someone typing their password.

- **Key Logging**
  An installed keylogger intercepts passwords as they are typed.

- **Searching**
  IT infrastructure can be searched for electronically stored password information.

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

- **Social Engineering**
  Attackers use social engineering techniques to trick people into revealing passwords.

...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.

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

- **Don’t store passwords in plain text format.**
- **Blacklist the most common password choices.**
- **Monitor failed login attempts... train users to report suspicious activity.**
- **Prioritise administrator and remote user accounts.**
- **Change all default vendor supplied passwords before devices or software are deployed.**

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.**

For more information go to [www.ncsc.gov.uk](http://www.ncsc.gov.uk)