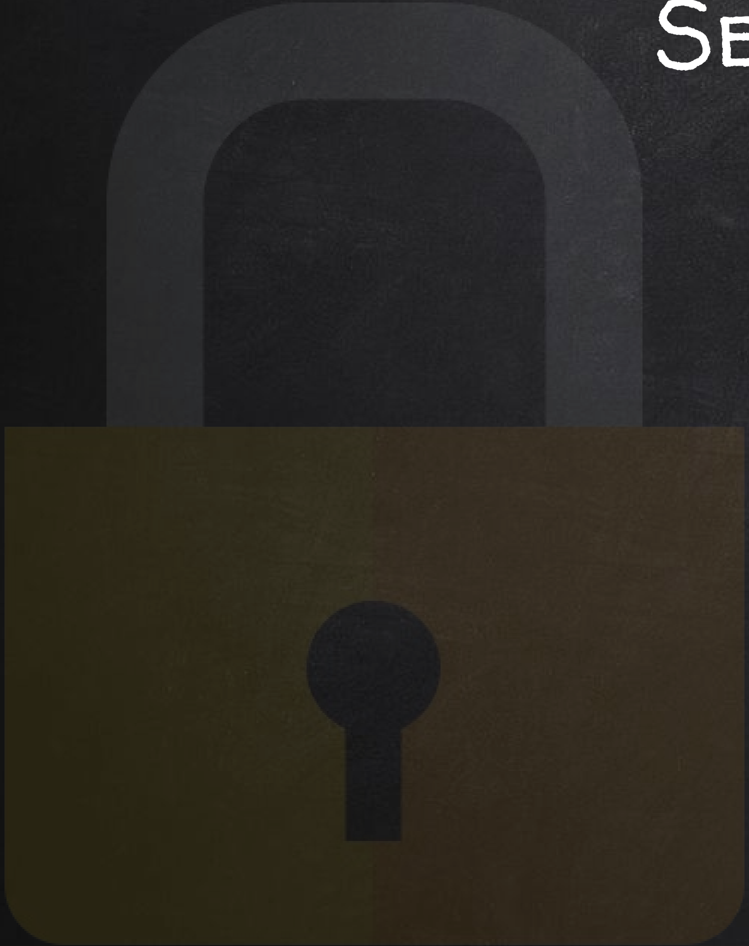
Security



Security

1. Captive Portals

- Open networks.
- No encryption is used.
- Lots of ways to get in.

Solution:

- Do not use captive portals.
- Use WPA/WPA2 enterprise instead.

Security

2. WEP

- Lots of methods to crack it.
- Even SKA networks can be cracked.

Solution:

- DO NOT USE WEP.

Security

3. WPS

- WPS pin is only 8 digits.
- Can be brute-forced even if the router locks.
- Then it can be used to get the WPA/WPA2 key.

Solution:

- Disable WPS.

Security

4. Advanced Wordlist attacks

- Work against all networks.
- Password can be cracked as long as it's in the wordlist.

Solution:

- Use long complex password of letters, numbers and symbols.

Security

5. Evil-Twin Attacks

- Exploit the users.
- Work against all networks.

Solution:

- Educate the users.
  - Always connect to the right AP.
  - Never enter password in a web interface.

Security

Summary

1. Do not use captive portals.
2. Never Use WEP.
3. Disable WPS.
4. Use WPA/WPA2 with a long complex password.
5. Educate users