Usability

❑ If we make security too hard, users will avoid it.

- Onerous password restrictions,
- Organisation resource restrictions with dummy codes need for workarounds.

❑ Workarounds:

- Shared logins, cloud storage, BYOD (iPads, phones),
- Social engineering attacks become easier.

What's Legal

- **Check your ISP's Acceptable use policy – it's in your contract.**
  - It may forbid hacking activities like port scanning.
  - Most hacking activities are covered by non-electronic crime laws.
  - Port scanning = trespass
  - Packet sniffing = privacy laws
  - Laws are constantly being updated to remove loopholes caused by new technology.
- **Laws are not consistent across Australia or the world.**
  - Makes enforcing difficult.

What's Legal

- **<u>Never</u> attempt to test a system unless you have express permission to do so from the owner of the system.**
  - Even then you may be breaking the law.
  - Be subtle. Don't break things. Be discreet.
  - Some changes to Australian law make it illegal for Sys Admins to test their own networks!
  - Never test cloud / live web services.
  - GET PERMISSION IN WRITING
- **Real black hats create a duplicate of the target system and practice on it.**
  - Build your own network and practice on it.

Testing security

❑ Social engineering

- A off-line activity used by hackers to trick network administrators and other staff into providing passwords, user names and access to secure systems.
- Activities include 'dumpster diving', phone calls and ‘pretexting’, shoulder surfing, tail-gating.

Testing security

❑ Penetration test

- "...a method of evaluating the security of a computer system or network by simulating an attack by a malicious user... " (Wikipedia*).
- Penetration testers may have some security product to sell, and may go to extreme lengths to compromise a system.

❑ Audit

- A program of activities including penetration testing, risk analysis, interviews with staff and reviews of hardware and software access.

Philosophies: TNO

- **“Trust no-one”.**
- **Steve Gibson’s philosophy on internet security.**
  - Encryption keys are only known to the sender and the recipient (NOT CAs, Skype, 3rd parties).
  - Peer to peer connections are NOT mediated by a central server.
  - Cloud storage providers CANNOT decrypt your stuff if compelled by governments, law enforcement.
  - TelCos (Telstra, Optus, ISPs) CANNOT intercept (proxy) your secure web and mail sessions.

Philosophies: PIE

- **“pre-internet encryption”.**
- **Steve Gibson’s philosophy on encryption.**
  - Encryption keys are only known to the sender and the recipient (TNO).
  - All encryption occurs on the end-point (the host you control)
  - All decryption occurs at the other endpoint (the host the recipient controls).
  - Good for secure comms., secure storage.