2.2.2 Model Acceptable Security Practices

Tommy Zumtobel

How to be safe on the web

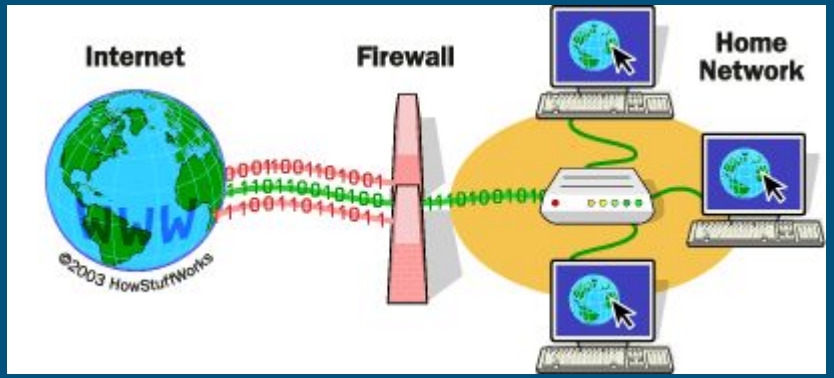
1. Install protective **software**.
2. Choose **strong** passwords.
3. BACK UP on a **regular** basis!
4. Control **access** to your machine.

Install protective software

When installed, the **software** should be set to scan your files and update your virus definitions on a regular basis.

This will help to keep **unauthorized** people from snooping around your computer when it's connected to the Internet.

Shut down or restart your computer at least weekly.



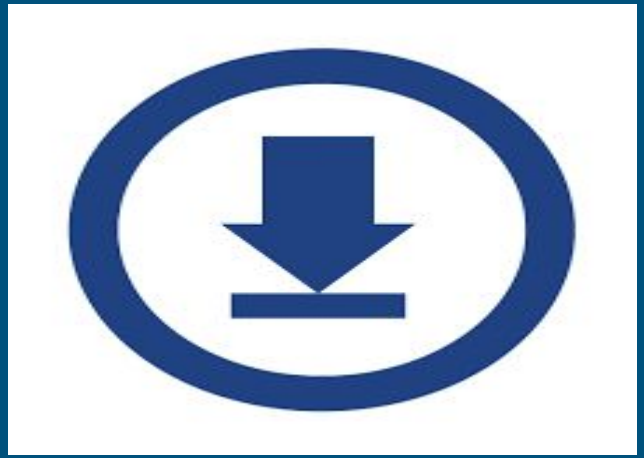
Choose strong passwords

- Strong passwords use a combination of letters, **numbers**, and special characters
- Create a different password for each important account, and change passwords **regularly**.
- Strong passwords are **less likely** to be hacked than very generic passwords.
- Be wary of using the **"save password"** option.
- Use **two-factor** options when available.

BACK UP

Regular, scheduled backups can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be **retrieved** if needed.

Its recommended that you store this information **securely** and even consider storing extra copies at another **location.**



Control access to your machine.

Don't leave your computer in an unsecured area, or unattended and logged on, especially in **public** places.

When leaving your computer unattended, lock it to prevent theft of the machine. We also suggest that users lock the screen with a password to **safeguard** data.

Video

Resources

http://www.foxnews.com/opinion/2011/10/29/10-tips-for-safe-computing.html

https://ist.mit.edu/security/tips

https://www.odu.edu/ts/security/awareness