Protecting your devices and network

Protecting your computing devices

**Your pc devices are the portal to your online life, storing a lot of your personal data**

**Therefore. Its important to protect the security of you devices**

- turn the firewall on

- **You should set up at least one type of firewall** (either software or hardware firewall)

- The firewall should be turned on and constantly updated to prevent hackers from accessing

your personal or organizational data

- install antivirus and antispyware

- to prevent this, you should only ever download software from trusted websites

- but you should always use antivirus software to provide another layer of protection

- manage your operating system and browser

- you should **set up the security settings on you computer and browser to medium lever or**

**Higher**

- **regularly update your computer**s operating system, including your web browser and

download the latest software patches and security updates from the vendors

- set up password protection

- **all your devices should have a password to prevent unauthorized access**

- **sensitive data should be encrypted**

Wireless network security at home

Hackers will be aware of the **PRESET SSID and default password** (of rooter) therefore it

**should be changed**

Further more you should encrypt wireless communication by **enabling wireless security and**

**the WPA2 encryption feature**

hackers can attacks with reinstallation attacks or (KRACKs) (breaking the encryption)

To mitigate this you should:  
 - update wireless capable devices

- Use wired connection for any device capable of it

- Use trusted virtual private network (VPN)

Public wi-fi risks

First of all **you should always verify that your device isnt configured with file and media**

**sharing and that it requires user authentication with encryption**

**Also use encrypted VPN**

Strong password

**Do not use dictionary words or names in any language**

**Do not use common misspellings of dictionary words**

**If possible use special characters [($%#@!^&\*()-…..)](mailto:($%#@!^&*()-…..))**

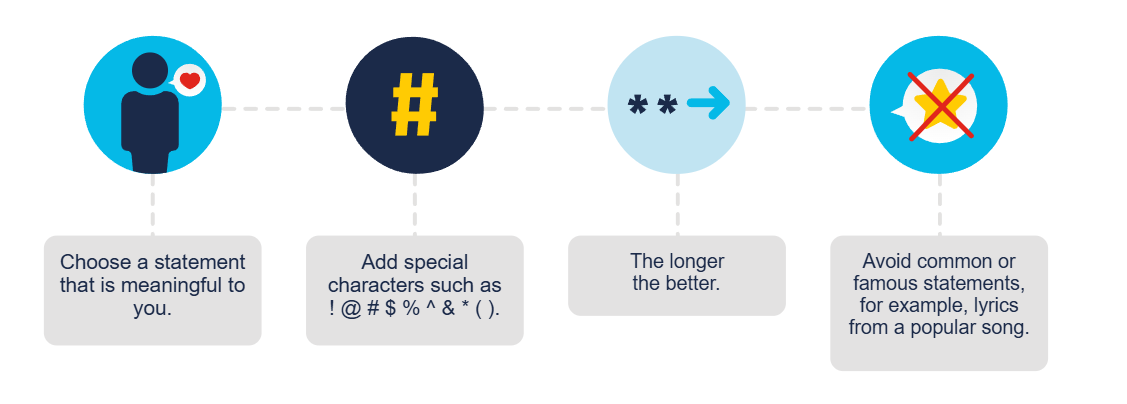
**Do not use computer names or account names**

**Use a password with more than ten characters**

Using a passphrase

Passphrase generally takes the form of a sentence (‘Acat [th@tlov3sd0gs.’)](mailto:th@tlov3sd0gs.’))

Making it easier for you to remember and its longer then typical password



Password guidelines

- Password should be at least 8 characters long but no longer than 64

- Common easily guessed passwords such as ‘password’ should be avoided

- Composition rules, such as having lower and uppercase letters and numbers

- Users should be able to see the password to improve accuracy

- All printing characters and spaces should be allowed

- No password hints

- No password expiration period

- No knowledge-based authorization, such as having to provide answers to secret questions

or verify transaction history