1. Install Anti-virus
2. Back-up regularly ( to another computer / cloud)
3. Configured Firewall
4. Password protect access
5. Strong Passwords

7 characters long – upper/lower symbols numbers – change regularly.

A strong password is a longer and more haphazard mixture of characters, like passphrases. Create a string of letters, numbers, and symbols, use words that make up a silly statement.

1. Use and check digital signatures(a digital code attached to message)
2. Use digital certificate
3. Data encryption
4. Use SSL (if necessary – can use https)
5. Good Staff Training
6. Use Authorised Personnel (WHO SHOULD KNOW):

* Principles of the Privacy Act 1988.
* Data protection and encryption.
* How to recognise and action phishing emails.
* Malicious intrusion of the system and programs.

***The above should be part of induction for new employees, with signed employment agreement.***

**2-Factor Authentication**

**Advantages**

The safest way to lock down your accounts with two-factor authentication is to employ a physical security key. It has been found in studies that security keys blocked 100 percent of bulk phishing and targeted attacks.

**Disadvantages**

Where the is a positive there is normally a negative. The negative of using a security key, is that if you ever break or lose the key you could be locked out of your system, and you will have to change your second-factor authentication method to a new key.

Sim swapping attacks.

**Encryption**

**Windows**

In Microsoft Windows.

1. A right click on a file or folder and select Properties.

2. Select the Advanced button and select the Encrypt contents to secure data check box.

3. Select OK to close the Advanced Attributes window, select Apply, and then select OK.

To encrypt a folder.

1. Create a folder you would like to encrypt.

2. Go to Disk Utility.

3. Click File > New Image > Image from Folder.

4. Find and click on the folder you created.

5. Select an encryption method, create a password, and save your encrypted folder.

**Hashing**

**MD5 - SHA**

Create a hash of a password and store the hash – not the password!

Use SHA not MD5

SHA – 512 most secure

**SALT** password from rainbow table by adding unique number to password

**HMAC**

**RIPEMD**