



# Security of your Data

# Why protect your data?

Data is the life blood of most businesses

Without the data on your system your business cannot make money, provide you (and maybe lots of other people) with a job

or at home, you could lose all your digital images!!

Data is one of a persons' or businesses' greatest assets

but ...  
disasters can happen ...

cyber-criminals love other people's data!

So .....



# What are the most common threats to any digitally stored data? How can I protect my digital data?

- Internet and email risks leading to virus or trojan attack
- Spyware
- Malicious script
- Natural disaster  
**also**
- Unauthorised access
- Power failure



# Use protection measures to protect the data on your computer system

1. Back up techniques
2. Virus protection
3. UPS or surge protector



# 1. Backup techniques

- Back-up is the computer term meaning to make a copy of any software **programs** which have been customised and any **data files** which have been created
- Why?
  - In case your hard disk fails eg from a power outage
  - In case your data is deleted by mistake (or deliberately)
  - In case of a virus attack
  - in case your building burns down
- What do you do with the backups?
  - Keep backups **securely off site** in an environment which has no heat, no moisture, no magnetic interference



# When should you do a backup?

- REGULARLY depending on how often you enter data
  - daily data entry would be backed up daily, weekly, monthly, yearly.
  - weekly data entry would be backed up every week, then every month, then at the end of the year



# How could you do a backup of your data?

- ☐ Computer
- ☐ Zip
- ☐ Cloning
- ☐ Backup and Restore
- ☐ Program commands
- ☐ Tape drives with special software and hardware
- ☐ Download apps or use settings on mobile digital devices

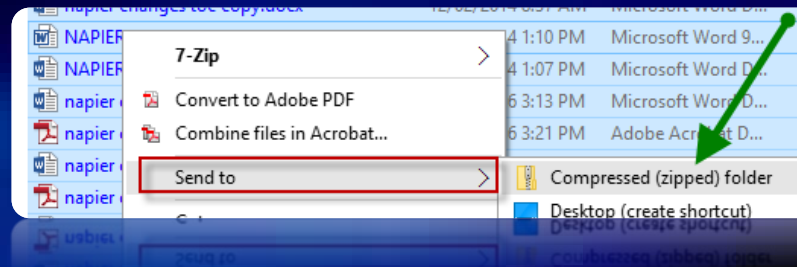


# Use Computer to copy files to an external storage source

- § Files stay the same
  - § Select them, copy them, paste them
- § Files can be transported to another site
- § Files can be transported to another PC



# Zip or compress files



- § Windows will compress multiple files or folders into one file (zipped) onto a USB stick, or external hard drive
- § Unzip will de-compress the files and folders or individual files
- § WINZIP is a graphical user interface (GUI) which has icons to make it easier to use



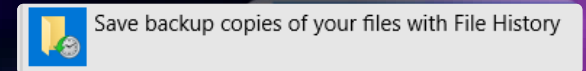
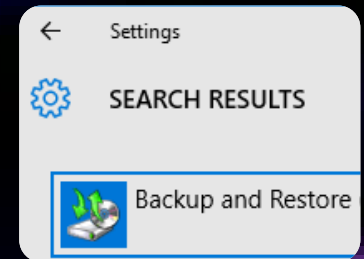
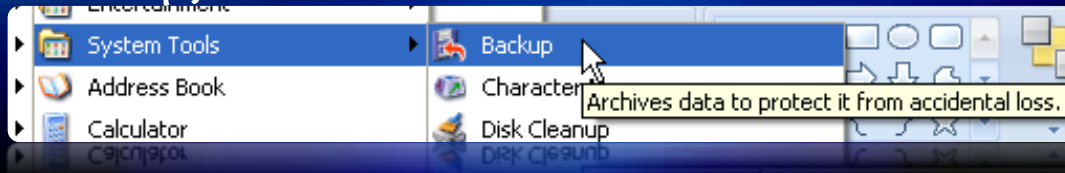
# Using cloning gadget from Inateck

- § Push a button and your drive will be cloned (totally copied) onto this gadget
- § Or choose to backup files only by using as an external hard drive



# Using Backup and Restore tools to backup hard drives

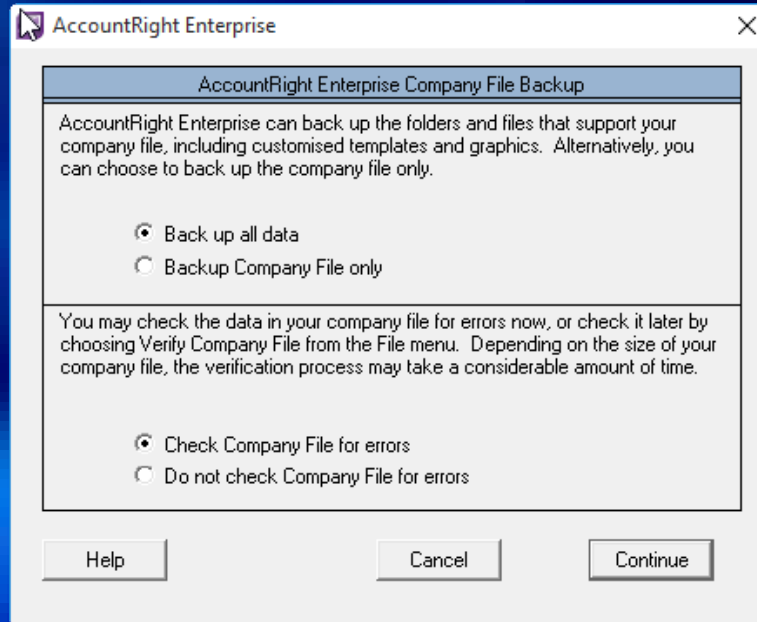
- § System tools (Win 7) Settings (Win10) used to backup hard disk drives (can back-up just data which has been changed since the last back-up)



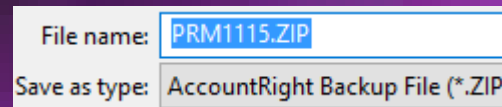
- § Backup tool will compress files (take out unnecessary spaces, convert formatting into coded commands etc)
- § When compressed, files cannot be used
- § Restore tool will de-compress files (put the spaces back in, convert the coded commands back into formatting etc). After restoring the files, they are able to be used

# Using Program commands

- § Accounting programs backup data entry whenever entry is made



- § Automatic name given to backup file – uses the date as the filename eg Nov 15



- § System crash or something goes wrong – just restore your backup of the data from the previous “correct” date

Procedure: At EIT, IT services works to ensure the integrity and reliability of data stored on the EIT network through the Institutes backup solution (tape back-up, automated to run every night).

## Use tape drives to backup network drives



- § Tape drives have specially designed software and hardware to back-up Network Drives
- § Tape drives are automated so that back-ups are done at night (no down-time for the customers or staff)
- § Tape drives are set to back-up all programs and data
- § Tape drives can be DLT (Digital Linear tapes) which back-up at 300 Mb/minute. Can hold up to 70Gig of compressed data.
- § Tape drives can also use DAT (Digital Analog tapes) which back-up at 100 Mb/minute. Smaller, can hold up to 20Gig compressed data.



# Backup your Android mobile device

§ You can download an **app** eg **MobiKin Assistant for Android**, and ensure you never lose contacts, text messages, apps, photos, music, videos and more. These will export to your computer

§ You can use your **phone settings** to access **Google backup** Backup & Reset. This has an option for backing up data, WiFi passwords, preferences and app data. This will be tied to your Google account


§ OR

§ You can use a **USB cable and your computer** – find the folders on your phone and copy and paste to your computer

More Info: <https://www.androidpit.com/how-to-back-up-everything-on-android>



# Back up your iPhone

- § You can purchase an app eg  which will save all your iPhone contacts on your Mac or PC just by drag and drop to your device. You can use this to sync your contacts between iPhone and iPad.

<https://imazing.com/features/>



- § You can backup using iCloud Backup. You can check your backup by choosing Manage Storage. This will tell you when your backup was made. This can be set to backup automatically.

You can also backup to iTunes.

This can also be used to backup your iPad or iPod touch

<https://support.apple.com/en-nz/HT203977>



# Online backup for all devices ..

- Go to <https://www.idrive.com/universal-online-backup>

Online Backup for All Your PCs, Macs, iPhones, iPads and Android devices into a single account



The image is a promotional graphic for IDrive. It features a desktop monitor, a laptop, a tablet, and a smartphone, all displaying the IDrive website. A large white cloud is positioned to the right, with several colorful icons (representing photos, documents, and applications) floating around it. A curved arrow points from the devices towards the cloud, symbolizing data backup. In the bottom right corner, there is a small video camera icon and the text 'Watch video', with a black arrow pointing towards it.

Watch video

- And watch the video

# Summary of back-up techniques

§ Back-up **regularly** depending on how often you enter data  
Back-up **program files** which have been **customised** and **data**

§ How?

- ☐ Computer for **files**
- ☐ Zip for **files and folders**
- ☐ Cloning for **hard disk drives**
- ☐ Backup and Restore for **hard disk drives**
- ☐ Program commands used to backup **daily data entry**
- ☐ Tape drives with special software and hardware for **network drives**
- ☐ Download apps or use settings on **mobile devices**
- ☐ Pay for **Online Cloud Backup**

§ Keep backups **securely off site to** prevent corruption of your  
when in storage

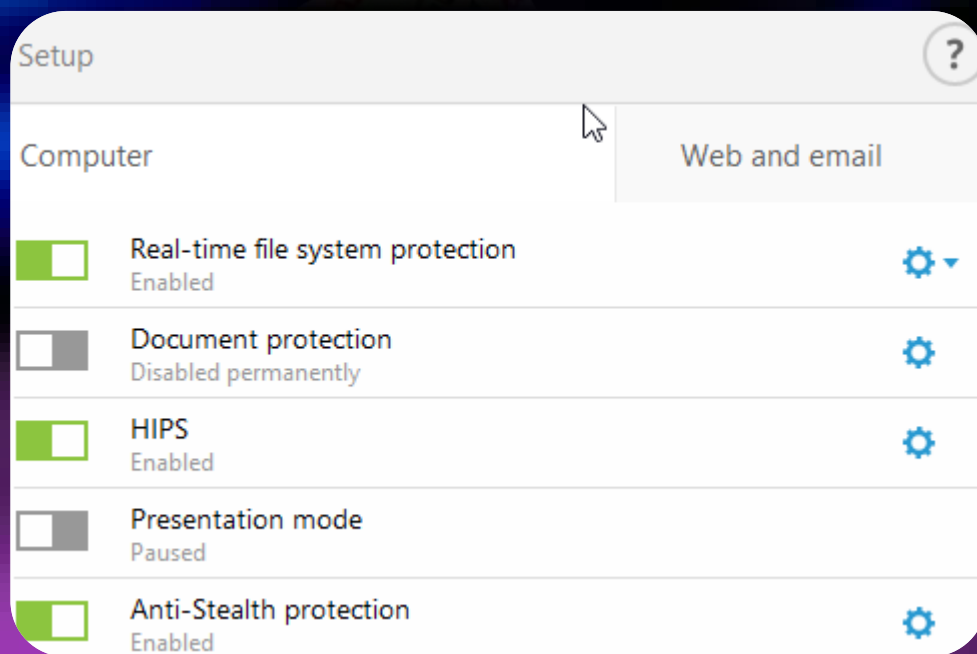


## 2. Virus protection measures

- Why do you run anti-virus software????

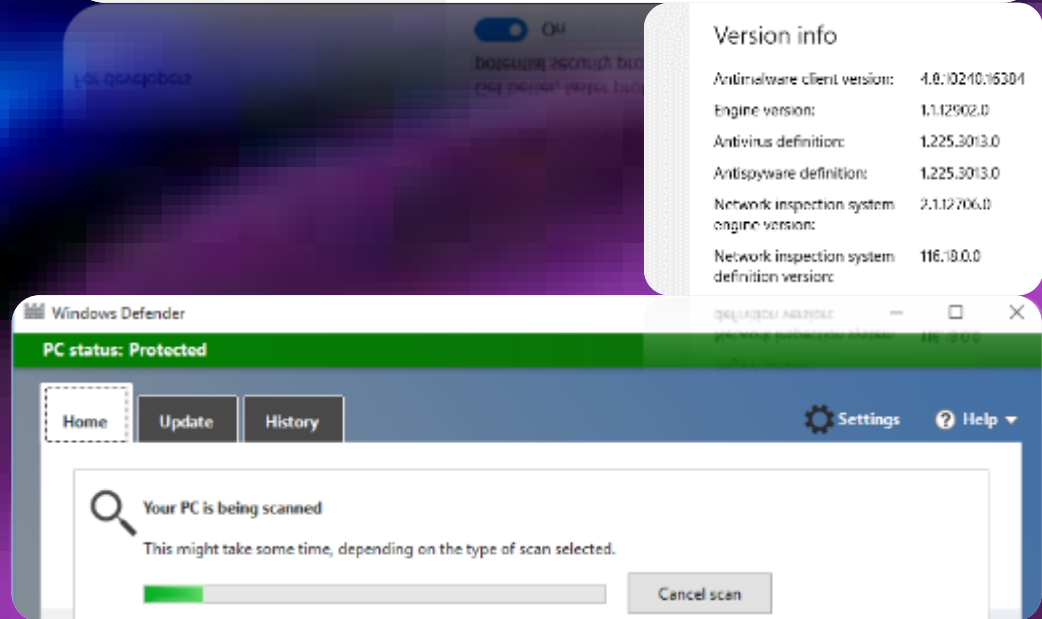
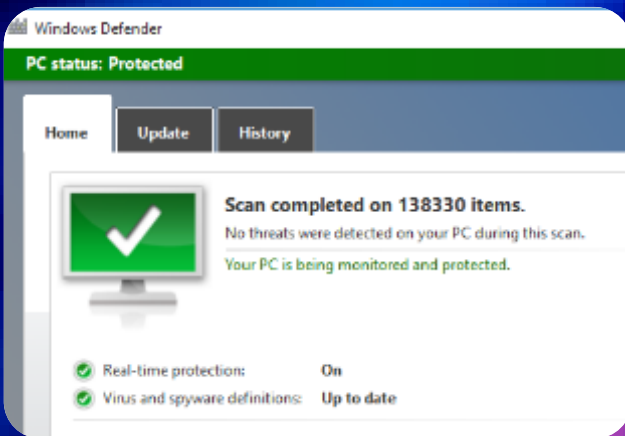
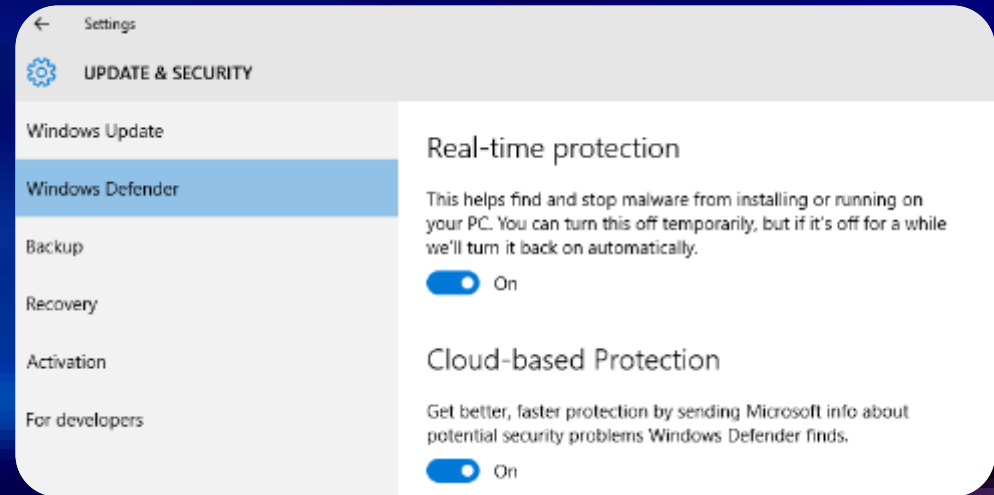
Because a virus attack

- Could destroy, scramble, rearrange your data
- Could destroy your motherboard
- Could delete system files
- Could format your HD



# Windows 10:

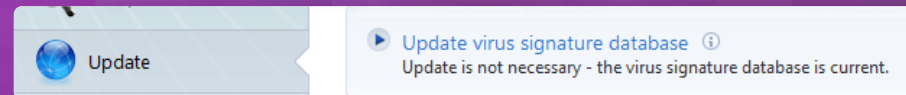
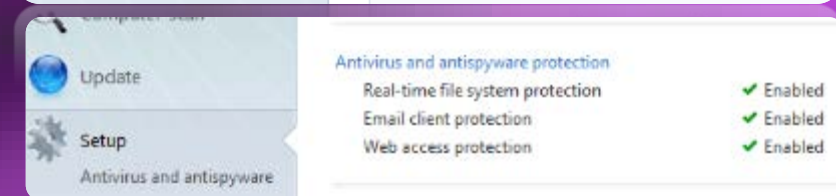
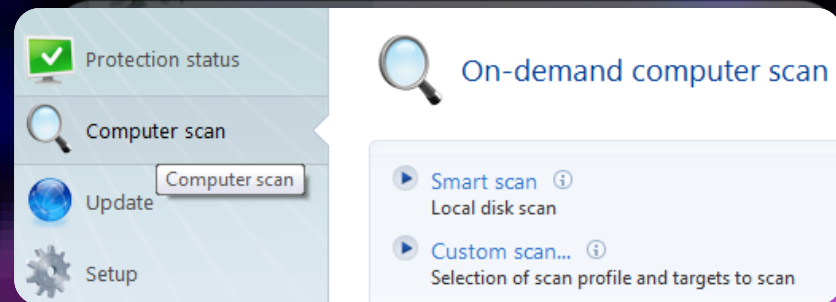
- Includes Windows Defender with Real-time protection
- Windows Updates the anti-virus software **REGULARLY**



# Windows 7

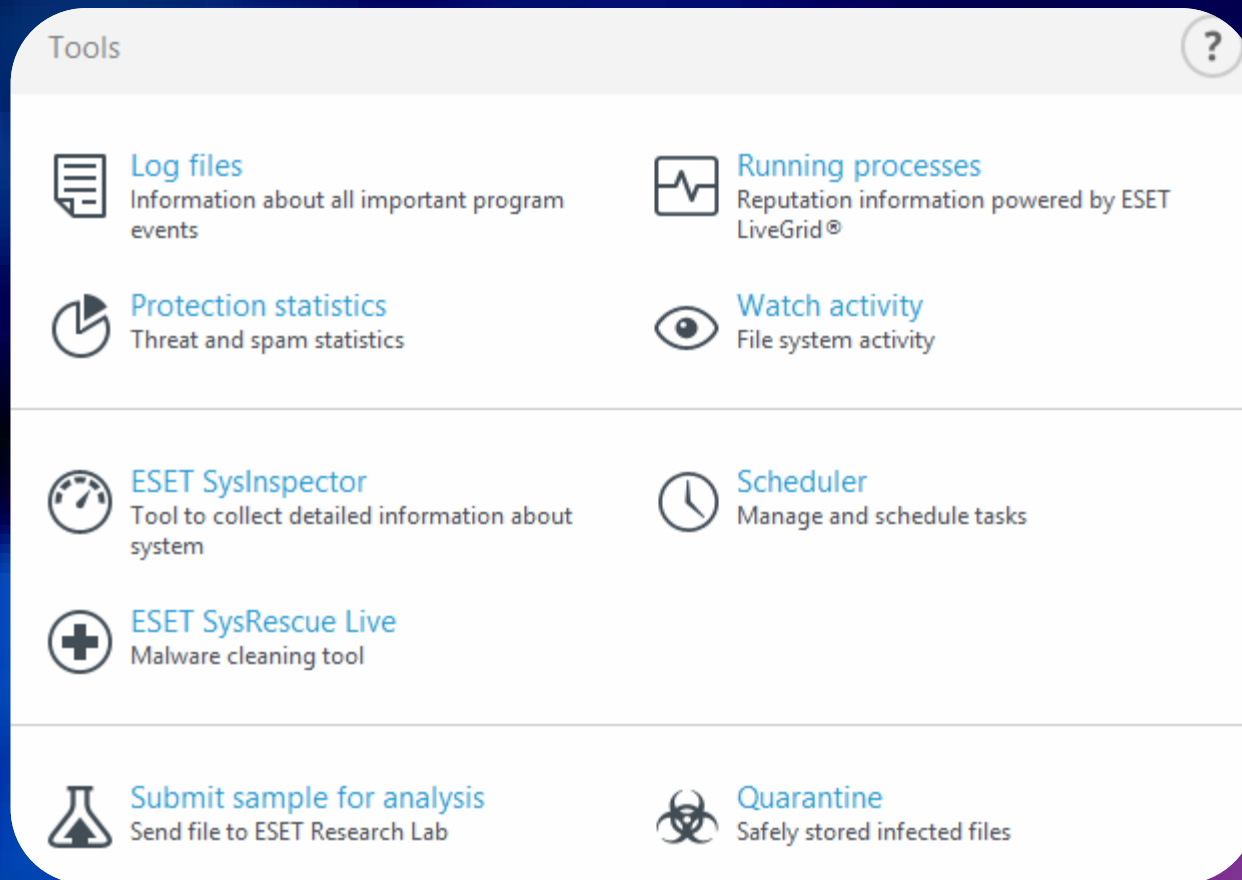
....

- Needs you to Install anti virus programs which RUN AUTOMATICALLY
- You need to update the anti-virus software REGULARLY
- Lots of free software available





- You can use Anti-virus software Tools to make sure the Virus Protection is doing what you want it to do



# Security procedures for you to consider at home

- Be informed!
- Don't open emails that look suspicious or are from unknown sources.
- Don't download or install programs from the Internet or other sources unless they have first been checked by your anti-virus scanner.
- Change your password regularly and avoid using easy to guess passwords such as family or pet names.
- Do not share your password with anyone.
- Get someone to look at your computer immediately you suspect your PC may be infected.

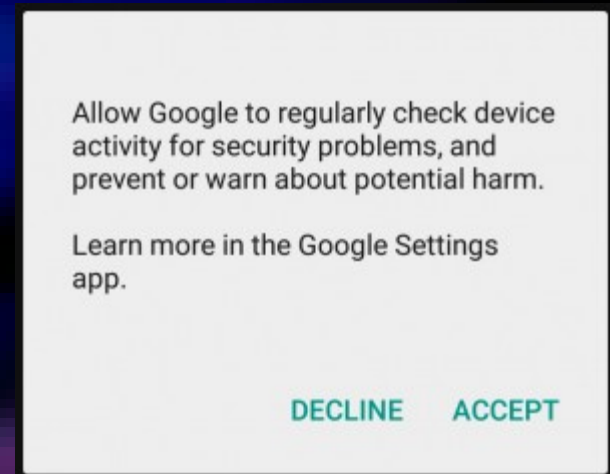
# iPad and iPhone



- iOS is designed and built to only accept and install software that has been approved by Apple so you don't need anti-virus software
- But ... **you need to keep your devices software updated!!**
- Note: old iOS devices operating software allowed the CIA to get data that has been given to WikiLeaks

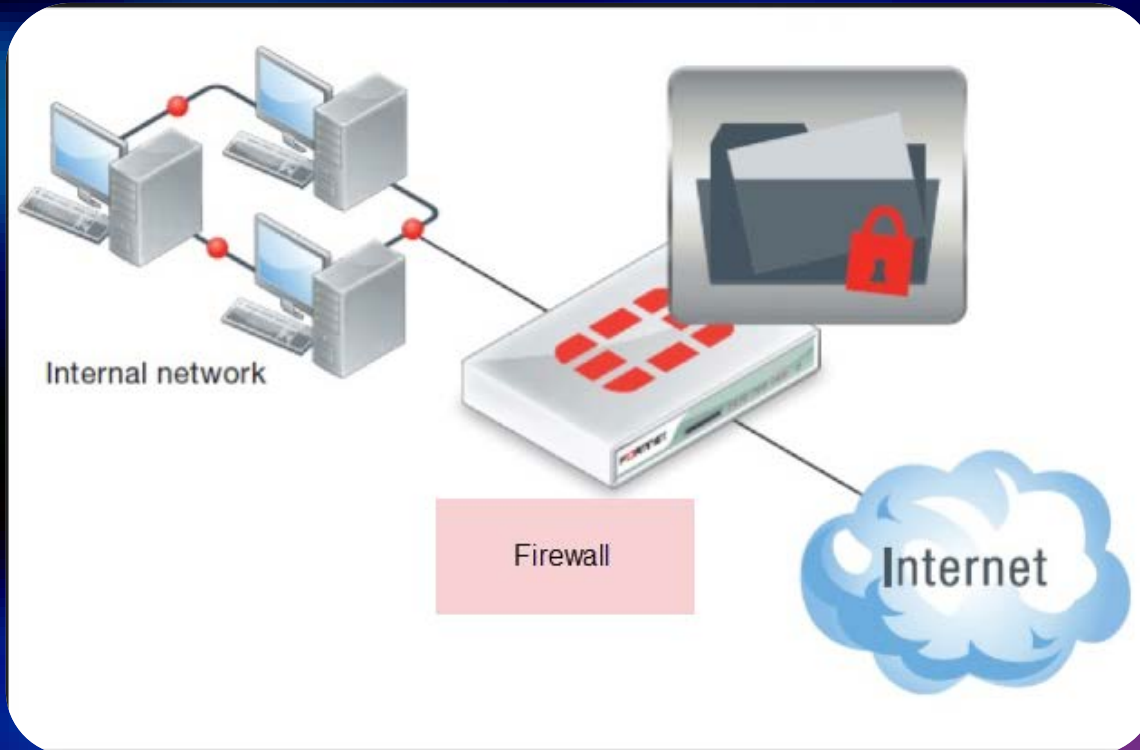
# Android devices

- Android has default security settings which allow Google to regularly check your device activity for security problems and prevent or warn about potential harm
- You should be careful about what you download making sure you install software apps from trustworthy places eg Google Play as apps could contain Malware
- Google recommends that Android users protect their devices with lock screens and PIN codes, and to enable a setting called [Verify Apps](#), which scans apps downloaded from outside of Google's app store for malware
- But ... **you need to keep your devices software updated!!**
- Note: old Android software allowed the CIA to get data that has been given to WikiLeaks



## Secondly ....

- Install a Firewall



Check the incomings and outgoings

Thousands of apps? Thousands of threats!

Want to know more? <http://www.howstuffworks.com/>

# What is a firewall?

- A software/hardware firewall controls the point of entry to your computer, device or network. A point of entry is called a Port. It is a barrier between the internet and your computer, device or network. Many mobile devices do not have firewalls to limit connections.
- When the firewall is installed, you set it to allow or reject certain types of data. The firewall then protects the network or PC from outside threat eg unauthorised access, virus, trojan attack. Note: at EIT .zip and .mdb files are blocked at the firewall.
- A firewall screens all outgoing data eg is the program authorised to access the internet (is this Spyware sending data out!!!)
- A firewall screens all incoming data eg is the source acceptable, is the type of data safe (depending on your settings).

Want more info? Go to [whatis.com](http://whatis.com)

# Web based applications ....

## Cloud based applications

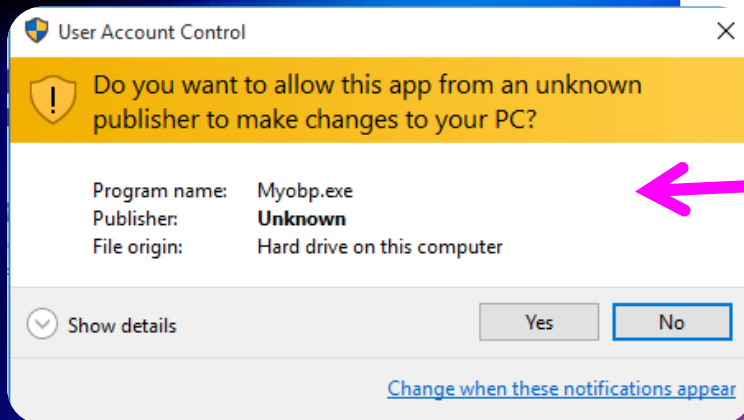
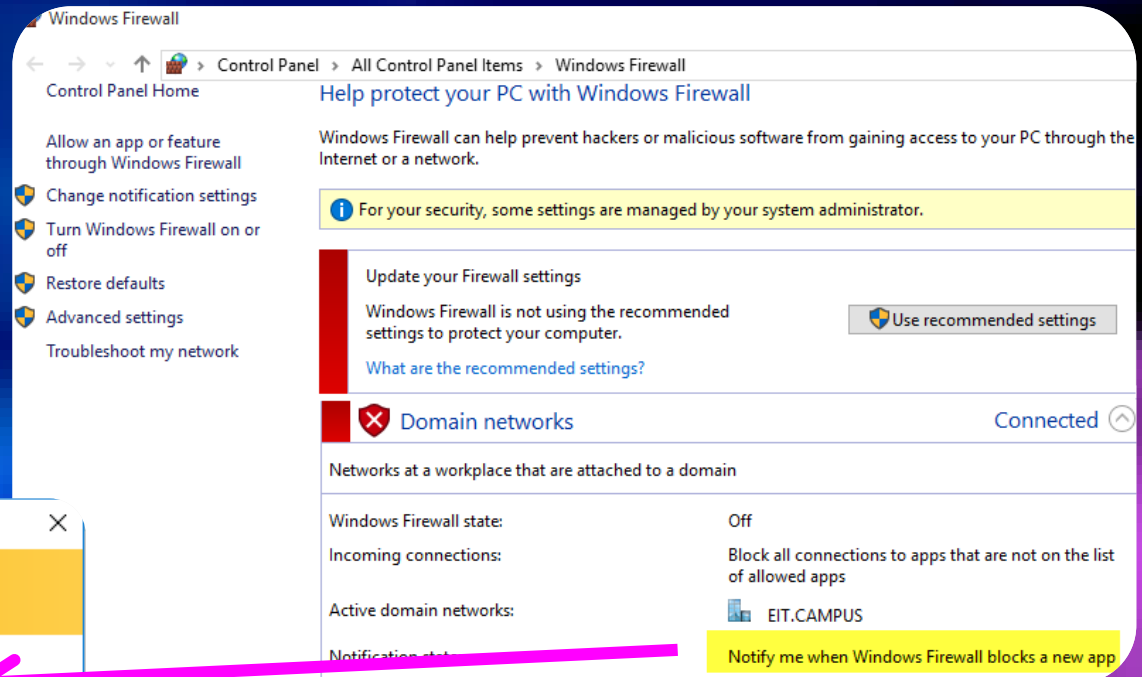


Security needs to follow data as it moves across the network or WiFi network on different devices



# Evidence of firewall working ...

- Features include logging and reporting, automatic alarms when there might be an attack.



# From Andrew Khan, Senior Business Manager, Ingram Micro New Zealand

- Customers, employees, contractors, and business partners all want to access critical business data and network resources. “The number and kinds of **devices** used to access this data are expanding rapidly, from **smartphones** and **tablets** to **personal laptops** that are increasingly not controlled by IT. At the same time, critical data is being **stored offsite** on a variety of third-party platforms, something known in the industry as Shadow IT.”
- “Traditional network perimeters are changing,” he continues. “Users expect to be able to **access any information, from any location, at any time, using any device**. But the imperative stays the same: you need to protect and preserve critical, sensitive or confidential data in the midst of a rapidly expanding environment where traditional security solutions are less and less relevant.”



<https://itbrief.co.nz/tag/ingram-micro-new-zealand/>

### 3. Power protection measures

- **Save, save, save**  
so that data in RAM (temporary storage)  
is saved to hard drive (permanent storage)
- Use an **Uninterruptible Power Supply (UPS)**  
this allows your computer or network to keep  
running for a short time when power is lost – has a  
battery that “kicks in” it allows you time to **save**  
**and exit** it can also filter out power fluctuations to  
prevent very costly damage to your data
- No UPS? Cheapest option is to plug the power  
cord into a **surge protector** Protectors can be very  
comprehensive expensive models or cheap and  
basic



# End of presentation

Next steps

Go back to the workbook

You will see that there are Study Notes on Security Risks for your data