




## Be safe when communicating online

A workshop for groups who use computers to communicate and are concerned about their security and safety on-line.



# Use a firewall

- A firewall acts as a barrier between the public internet and your private computer or network and blocks threats including some viruses.
- A firewall protects you against a number of different online threats:
  - Hackers breaking into your computer.
  - Some viruses, called “worms,” that spread from computer to computer over the internet.
  - Some firewalls block outgoing traffic that might originate from a virus infection.

# A Firewall does not...

- If you give permission for other computers to connect to yours.
- If it is switched off, disabled or contains many exceptions or open ports.
- Against most viruses.
- Against spam.
- Against spyware installations.
- Against any kind of fraud or criminal activity online.
- If you or a virus has created a back door through the firewall.
- If a hacker has the password for the firewall.
- Against people with physical access to your computer or network.
- Against malicious traffic that does not travel through it, for example via a poorly configured wireless network.
- Against attacks after a network has been compromised.
- Against traffic that appears to be legitimate.

# Install a firewall...

- There are several firewalls available, for this workshop, we will use Zone Alarm.

# Prevent virus infections

- Anti-virus software is one of the main defenses against online problems. It continually scans for viruses, including Trojans and worms. To be effective it must be kept up-to-date.
- Being infected by a virus can have very serious consequences including:
  - Identity theft.
  - Fraud.
  - Loss of data.
  - A slow or unusable computer.

# What anti-virus software does NOT do

- Anti-virus software will not protect you against:
  - Viruses for which it has no signature.
  - Programs that you choose to install that may contain unwanted features.
  - Most Spyware.
  - Spam.
  - Against any kind of fraud or criminal activity online.
  - A hacker trying break into your computer over the internet.
  - It is not effective if it is switched off for any reason.

# Install anti virus protection

- There are several anti virus programs available, for this workshop, we will use AVG anti virus.

# Don't let strangers get inside your computer

- Spyware is an insidious threat to privacy and can result in financial fraud. It is also a huge pain to live with.
- There are different types of spyware. Some adware is designed to get you to visit commercial websites, typically for gambling and porn. Surveillance Spyware is the most extreme version which may Scan your hard disk for private data such as credit card numbers.

# Install Spyware detection software

- There are several Spyware detection programs available, for this workshop, we will use Microsoft Anti Spyware (Beta).

# Keep your applications and operating system fit and healthy

- As new threats emerge, Microsoft updates its Windows operating system and Microsoft Office applications to block them. However, you need to download the updates regularly to be sure of getting maximum protection.

# Check for Updates!

- Its easy! Just visit the website...
- [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)
- <http://office.microsoft.com/en-us/officeupdate/default.aspx>

# Resources!

- There are a huge amount of resources available online, Three that we like are:
- <http://www.getsafeonline.org/>
- <http://www.itsafe.gov.uk/>
- <http://www.banksafeonline.org.uk/>