Internet Security

An Illawarra Prayer Network member had a computer hacked whereby someone was able to record conversations in her house via the in-built computer microphone. One particular conversation was recorded, whilst the computer was on, and then sent to her mobile phone, as a voice message. On another occasion, the hacker using a "Keylogger", was able to type a message, which was viewed on the computer screen under the browser address. The webcam had also been compromised.

Take the following preventative helpful actions:

1. Disable computer microphone when not in use i.e. Control Panel - Sound - Recording - Internal Mic - Disable - Apply – OK.

2. Cover webcams when not in use, with either shutter or black adhesive tape.

3. Ensure Internet Browser does not redirect to unsecured websites (for Firefox users, go to Settings, General tab and check box "warn me when web sites try to redirect or reload the page").

4. Delete browsing history, temporary files, cookies etc.

5. Have an Internet firewall (and for additional protection, restrict connected computers to named devices only).

6. Keep antivirus software up to date and regularly run scans or other virus/malware programs.

7. To remove hyperlinks embedded in documents right click on the hyperlink and select “remove hyperlink”.

8. Recommend removing author identity information from your document properties before placing the document on the Internet.

More detailed information about the prayer member's cyber attack experience and subsequent police investigation will be made available soon on the 5ICM website.