



Library recommended WiFi safety tips

Information passing through the Library's wireless access service (with the exception of your initial logon using borrower number and PIN and secured sites which use https) is not secured and could be monitored, captured, or altered by others. There are risks involved with connecting to a public wireless connection, such as possible viruses, malware, loss of data, possible hacking/snooping by others connected, possible hardware/software failure. It is your sole responsibility to protect your information from all risks associated with using the Internet, including any damage, loss, or theft that may occur as a result of your use of the Library's wireless access.

To help ensure your security, the library recommends these safety tips:

- Make sure you're connected to a legitimate wireless access point. If in doubt, please check with library staff for the SSID of the library WiFi network.
- Use current legitimate anti-virus and anti-malware (anti-spyware) software with updated definition files.
- Keep your operating system regularly updated with all available security patches.
- Enable (or install, if needed) legitimate personal firewall software for your computer.
- When using web services (including anything you would log into such as webmail, financial sites, and others), ensure that the site requires a secure login. Secure logins use the "https" protocol, and are generally indicated by a "lock" icon displayed in your web browser. Secure site logins help prevent electronic eavesdroppers from learning your username and password.
- Encrypt files before transferring or emailing them.
- Use a virtual private network (VPN) if possible.
- Be aware of people around you.
- Turn off file sharing.
- Password-protect your computer and important files.
- When setting up the WiFi connection with the library always choose "Public Network". Network discovery is turned off by default so other users cannot see your computer.

