

Some Helpful Tips for Safe Computing

It's important to keep your computer reasonably secure while using the Lemurian Fellowship's online course, especially when sending or receiving confidential information. Here are a few tips recommended by computer professionals:

Keep your computer operating system and browser current, especially the security updates. Research anti-virus, anti-spyware and other malware protection software, and install if needed.

Use the firewall protection software that you purchase or was included with your operating system. Check with its manufacturer or consult knowledgeable sources for recommended firewall settings.

We do not recommend doing student work on public computers such as Wi-Fi hotspots at coffee shops, airports, hotels, etc. If you are using a library computer, ask the librarian if the computer is safe to use for confidential information.

If you use a shared computer to do student work, we recommend setting up your own individual account and password. Even with a separate account, it's good practice to clear your browsing session: log off completely, delete temporary internet files, clear your browsing history, and close your browser software. If your browser has an "auto-fill" feature, do not allow it to remember your user name and password. You may want to disable the "auto-fill" feature. Also, because an office or work computer is not completely private, we do not recommend using it for your student work.

Do not provide personal information except through our online course's secure messaging service or through the U.S. Postal Service. Our secure messaging service is encrypted e-mail which uses the Secure Sockets Layer (SSL) system. All data stored on our system is also encrypted. You can check if the website you're visiting is using SSL by looking for and clicking on a padlock icon in your browser window. Make sure that the URL on the certificate matches the URL of the page you are viewing.

We will never ask you for your password or personal information by telephone, standard e-mail, or text message. Do not use standard e-mail for confidential information. Keep your student log-in ID and password in a secure place. Change your password from time to time. Use combinations of letters (lower and upper case), numbers, and special characters like pound (#) or asterisk (*).