How To Protect Yourself Online

The following are general steps to take to ensure your online security is optimised.

Login details

Keep your login details secure. Do not write them down or tell anyone what they are, including the administration staff at Lion Health.

Passwords

Use strong passwords. Remember to make them unique so they cannot be easily guessed by someone else. They should always contain a mix of letters and numbers. Try to avoid using common phrases or anything obvious like your name or date of birth. Change your password regularly; we suggest that you do this at least once every three months.

Unsolicited emails

Be suspicious of unsolicited emails, even if they look like they're from a trusted source. Lion Health may communicate with you regarding this project using our NHS.net account.

Anti-virus software

Make sure your computer has anti-virus and anti-spyware software, and that it is continually updated allowing it to check the contents of the files on your computer against the information it holds about known viruses.

Personal firewall and secure wireless network

Make sure any computer which connects to the internet has appropriate firewall protection to block any unauthorised connections being made. If you're using a wireless network, ensure it is secure.

Update your web browser

Use the most up to date version of your preferred web browser, this could reduce your chance of falling victim to online phishing scams, by displaying messages to alert you.

Keep your operating system up to date

Make sure you download and install updates regularly.

Social Networking

Please be careful about the detail you provide when social networking. Never disclose personal information.

Sensitive information

Never enter sensitive information such as account details, PINs or passwords via a website link within an email.

Secure websites

Ensure websites are secure - look for the prefix 'https' and a locked padlock or unbroken key symbol. Check the authenticity of a secure website by double clicking on the symbol.

Contact the website owner on a known or independently verified phone number.

Attachments and emails

Beware of attachments and emails - even if they appear innocent, they could contain a virus designed to steal your personal information.

Bogus websites

Type the full address of secure websites into your browser, rather than searching for it - this helps avoid being misdirected to a bogus site.