**Phishing Protection for Lions**

At Lions Clubs International, we pride ourselves in service to others. Our efforts bring notoriety and respect from communities worldwide.  Unfortunately, this notoriety can also attract individuals that misrepresent themselves in order to gain access to personal or financial information. When individuals use the internet or phone to commit this type of fraud it is commonly known as “phishing.”

LCI systems are password protected for your safety and restrict access to personal information including email addresses and phone numbers. Outside of our LCI systems, Club information is widely known in our local communities through the media or non-LCI websites, and it is quite easy to obtain. This visibility also increases the chance of being contacted by a phisher.

**To protect yourself, your club, and the Association from phishing:**

* As a general practice when receiving unsolicited emails, do not follow embedded links in emails, especially if there is any mention of updating credit card information, personal data, PIN numbers, or passwords.  Delete these emails immediately.
* If you should be redirected to a website, verify that the URL address starts with https://.  The single letter S after http indicates that it is a secure site, and is likely legitimate. If the URL is not secure, close your browser immediately.
* If contacted by another club member or the Association Headquarters via email, mobile text message or social media, and there is a request for financial assistance, wire transfer, etc. do not reply to the message.  Contact the club member or Association staff separately via email, phone, or through the MyLCI Communications Center to validate that the request is legitimate.
* Always use virus protection software on your PC or MAC.
* Exercise caution when using public Wi-Fi systems in a coffee house, restaurant, or internet café.  These public systems offer no protection from unauthorized fraudulent monitoring.
* Create strong passwords for your email, social media, and other online accounts, and update your passwords often.
* Never store passwords, banking information, or credit card numbers in your email.