Lions Clubs International

LIONS CLUBS & CYBERSECURITY IN A VIRTUAL ENVIRONMENT

Lions Clubs of District 20-W // Avoiding E-Mail Scams

Increase in Cybersecurity Threats

In recent months, e-mail scams and other forms of cybersecurity attacks have become more prevalent because of the pandemic. As more business is being carried out using virtual methods such as e-mail correspondence and virtual meetings, new cybersecurity risks and threats have emerged. In the last week, we have seen increased e-mail scams circulating in District 20-W. Member awareness and education is more important now than ever to avoid falling victim to these attacks.

E-mail Imposter and Gift Card Scams

The most common scam that has been observed by IT cybersecurity teams are e-mail scams where bad actors create e-mail accounts that impersonate and pose as high-ranking individuals within an organization. In Lions Clubs, these are generally individuals like the district governor, vice district governor, and club presidents. The bad actor will ask the recipients of the scam e-mail if they are available and to do them a favor of buying gift cards and sending them the gift card information. Due to many Lions personal information being publicly available on Lions Clubs websites, it is very easy for these bad actors to identify high-ranking members and begin sending the scam e-mails to other members within a district or club.

How to Avoid These E-mail Scams

There are many ways to avoid e-mail scams like the one mentioned above. Here are several tips to avoid these e-mail scams:

- **Always double check the e-mail address of the sender** – Usually the scammer will create a new e-mail account and set their display name to impersonate a high-ranking individual. Depending on your e-mail client, you may need to click or hover over their display name but be sure to double check the email address of the sender. In most scam attempts, the e-mail address of the individual who is being impersonated will not match their primary e-mail address that you should be familiar with.
- **Do not open any attachments or click any links** – If you receive an unexpected e-mail with attachments or links, do not open them or click on them. Always contact the sender via phone or in-person and double check with them that they did in fact send you an attachment or link before opening them. Be especially cautious of shortened URLs that use services like tinyurl or bit.ly.
- **Be aware of generic greetings, misspelling, and improper grammar** – Many times scam e-mails will have generic greetings that do not directly address the recipient, misspelling, and improper grammar. These can all be signs that an e-mail is fraudulent.
- **Contact the individual you believe sent you the e-mail** – Speak to the individual that sent you the e-mail either by phone or in-person to verify that the e-mail is genuine and that they sent the e-mail to you. Verify the authenticity of requests, especially when you are being asked to buy something.

By: Lion Joseph Wagner – Saratoga Springs Lions Club
jwagner@saratogaspringslions.com

02/21