USEA SPAM & Phishing Policy FAQs

What is SPAM?

A SPAM email is unsolicited, bulk email designed to promote goods and/or services that may or may not be legitimate.

What is Phishing?

An email designed to acquire information such as usernames, passwords, and financial details by masquerading as a trustworthy sender. Successful Phishing attacks can cause financial loss for victims and put their personal information at risk.

How can I identify a Phishing scam?

The first rule to remember: Never give out any personal information in email. No credible institution should ever ask for this information via email, as email is inherently insecure. It may not always be easy to tell whether an email or website is legitimate, but there are many tools to help find out.

Phishing messages are more serious and may be difficult to identify. One of the first things to look at is the 'From' header. Below is an example of a poorly crafted email; it shows as being received from United States Eventing Association but the actual address from where it was received is: mailto:informative1@comcast.net

> ***From:*** *United States Eventing Association [mailto:informative1@comcast.net]*
> ***Sent:*** *Monday, October 23, 2017 8:23 AM*
> ***Subject:*** *IMPORTANT*
>
> *This message attachment and information is directed to the members of United States Eventing Association (USEA) only. This is a vital update and we are all excited about the coming days. Do have a nice day.*

Also consider the tone of the content, as scams generally contain the following:

- Alarmist messages and threats of account closures.
- Promises of money for little or no effort.
- Deals that sound too good to be true.
- Requests to donate to a charitable organization after a disaster that has been in the news.
- Bad grammar and misspellings.

Beware of the sense of urgency: emails with instructions to click a link to update your information should be considered suspicious. Typically, they are crafted with such wording to not allow the recipient time to verify the legitimacy. Example are: *'You must update your information immediately or your account will be locked.'* or, *'If your account is not updated within 24 hours your account will be closed'*. Legitimate emails rarely include such timeframes.

If you are concerned enough, contact the company that the email is purporting to come from by going to their website directly and finding the general customer service number (DO NOT use the contact information given in the email).

What should I do when I receive a suspected SPAM or Phishing email that appears to originate from the USEA?

When you receive messages that you believe are SPAM or phishing, these messages should **NOT** be responded to and links within these messages should **NOT** be followed. Below are the methods to report SPAM or phishing emails to the USEA. After reporting, the messages can be safely deleted.

- **SPAM**: Forward these messages **as attachments** to spam@useventing.com and to your email provider.
- **PHISHING**: Forward these messages **as attachments** to phish@useventing.com and to your email provider.

Contacting your email provider is always best, as they will directly report these to national and global SPAM and Phishing tracking databases that helps block future bad emails.

How do I send an email as an attachment?

Use the link for an excellent tutorial on the popular site LifeHacker.com for forwarding an email as an attachment for common email providers.

https://lifehacker.com/5803366/how-to-send-an-email-with-an-attachment-for-beginners