How to Spot a Scam

Communications and Public Relations is important in our club world. However, we need to worry about what the "bad guys" are searching for and sending us in order to get into our email and website.

Spamming is an unsolicited email. It is often an advertisement, a subscription offer, or a newsletter. They are annoying, but they are typically harmless. Just do not open them.

Phishing is an attempt to gather your personal information, passwords, etc. They are vague or they will warn you that something good or bad will happen to you if you do not respond. They may pretend to be from a commonly used company or service -UPS, FedEx, Amazon, Chase Bank. They will often times have some form of bad grammar as a clue to them not being legitimate. It may also have links that redirect you to fake data gathering web pages. They also commonly use classified ads, such as Craig's List to start an interaction with you.

Hacked is when an unauthorized user(s) attempt/s to access your account. Some signs may be that the contacts say they are receiving emails from you, or you start receiving mail delivery failures. There can be messages in your "Sent folder" that you did not send and there can also be activity pages/logs show logins from places and times you did not do.

Spoofed is when someone sends an email with your name in the "From" field using an account that is not associated with you. Some signs that this is happening may be that your name is John Doe and your email address is johndoe@gmail.com, but people are receiving emails that show "John Doe" as the from name, but the email address shown isn't johndoe@gmail.com.

A simple click can cost you a lot and make you frustrated.

Tips:

Below are common indicators that a message may be nefarious - plus some tips to help you avoid being a victim:

- Look for tell-tale signs an email is a scam, such as:
  - Information you did not request and are not expecting
  - From someone you know (or in your workplace), but with an unusual or unexpected request
  - Uncharacteristic writing style for the person who purportedly sent you the email
  - Asks for personal or sensitive information – unexpectedly
  - Asks for money – usually to be wired or to get buy gift cards
  - Asks for highly confidential information – like W-2s or passwords

    - The email address does not match the expected address. For example: Email From says “John Doe” but when looking at the email address, it is “john2354642@ gmail.com” and not the expected johndoe@companyname.com address
    - Alarmist statements and threats of account closures or arrest
    - 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
    - Misspelled words or poor grammar
    - Something just seems off or odd – your gut is telling you this email is suspicious
- Do not click on links within an email. It is best to use your web browser to navigate to the desired website by typing in a known website address yourself.
- Some trusted senders have had their mail accounts hacked. If you suspect something odd in the email exchange, contact the sender directly to verify a message’s legitimacy – remember to use a phone number from your contacts rather than the number that may be listed in the email. For example, if you get a notice about your bank account, call the number on the back of your debit card rather than clicking the link or calling the number in the email.
- Someone leaves an incoherent voicemail from an unknown number. This is probably a scam trying to get you to call back. Do not call back any unknown numbers.
- Someone calls or leaves a voice message and says the IRS (or some other government agency) is coming to arrest you for a delinquent fees or taxes. This is a scam; if in doubt, call the IRS number found on the IRS website or visit the local IRS office.

Sources:

Patti Poe - GFWC CPR Committee

Marian St. Clair – GFWC President Elect

January 11, 2020