Email Spoofing – A 2022 Association Chapter Update

A few years back, we wrote a post on email spoofing and association chapters -- what it is and how chapters and members can keep themselves safe from it. We've been asked recently to provide updated guidance, as hackers get sneakier and find ways around the guardrails many association chapters put in place.

94 percent of all malware (software designed to disrupt, damage, or gain unauthorized access to a computer system) gets to a computer via email. All it takes is one click on a dangerous link. Even if you think you think you're safe, it's probably time for some reminders and some new association chapter email spoofing guardrails. Here are a few things to keep in mind and share with your members.

Email spoofing and phishing – what's the connection?

Email spoofing occurs when scammers forge the sending details on a message. They send an email from an address that looks incredibly like one you're familiar with, but with a small difference – like an added number or a misspelling. Spammers are hoping you won't take the time to notice the difference.

You see an association chapter email, assume it's from your organization and click on the link or open the attachment. That's when spoofing turns into phishing, as hackers embed the spoofed email with malicious links or an attachment that installs malware onto your computer.

The latest phishing and spoofing trends

Email spoofing and phishing increased by 220% in 2021, as cybercriminals continue to take advantage of opportunities to spoof emails and phish for valuable information and credentials. And, an early 2022 review of trends identified ways the cyber threat landscape has changed.

File extensions: The most popular spoofing file extension used in Q1 2022 was .pdf, followed by .html and .htm. PDF files and .html extensions made up over 30% of used file extensions.

Credential phishing: Google, Adobe and Sharepoint were among the top ten .com domains used for credential phishing, which is a process spammers use to obtain login information.

Tax season scams: Early 2022 saw activity from the Emotet botnet, with impersonations of the Internal Revenue Service (IRS) targeting U.S. taxpayers, using fake W-9 forms to infect victims' devices.

Education is the critical first step

The association chapter spoofing security recommendations we made in our original email – related to SPF records and SPF checking and using a secure email provider -- are still important. Even more important is continual education for everyone connected to your chapter – members, volunteers, board members, sponsors, vendors, etc. The easiest targets are often those who aren't educated about the risks of spoofing and phishing.

Share these ideas with members, in your regular meetings, virtual chapter lunch and learns, special in-person chapter events, and your association chapter newsletter. Consider sharing it in multiple ways, as reinforcement is necessary for staying ahead of scammers.

Check the sender's information carefully

Checking the email header is one of the best ways to tell if an email isn't from where it seems. The header contains information including the email address and the sender's IP address, path of the email, recipient, subject, date, etc. Provide your correct sending information, so everyone knows what to look for.

Check the body of the email

And the email subject line. The email may look like your chapter's regular emails with no immediate red flags. However successful attacks are based on trust. Explain to members the importance of being wary of things like:

- Requests for a quick financial transaction, an e-signature, or sensitive information, and an urgency to open an attachment or click on a link
- Information that one can easily find on social media
- Spelling or grammar mistakes
- Subject lines suggesting a time-sensitive matter (e.g., "Hurry," "before it's too late," "expires on," "we need your help right away")
- Invitations to events or to collect rewards/promotions, especially if the email is one, they've already received

Recognize potential spoofing emails. Spoofing can include a request to:

- Click on a link. Before you click, hover over the link with your cursor to see the real link
- Transfer funds
- Provide information the "sender" should already have, like account information, social security numbers, etc.
- Provide a login or password over email

Provide a straightforward way to report potential scams.

Set up an email address and ask members to forward concerning emails. Remind them it's there and that you respond within X hours. (Be sure there is a volunteer monitoring your Inbox for these.)

Share strategies members can use to protect themselves. Share things like:

- What you won't ask for in email, like account numbers, social security numbers, etc.
- Consider not using a password manager to store and autofill login credentials and passwords
- Set spam filters a little stronger, so more emails go to spam
- Learn to use a browser's security features
- Keep antivirus software up to date

As technology continues to improve, and as more of us rely more on digital technology, association chapters need to stay on top of the evolving spoofing and phishing landscapes. Education from association can go a long way toward keeping everyone a little, or a lot, safer.