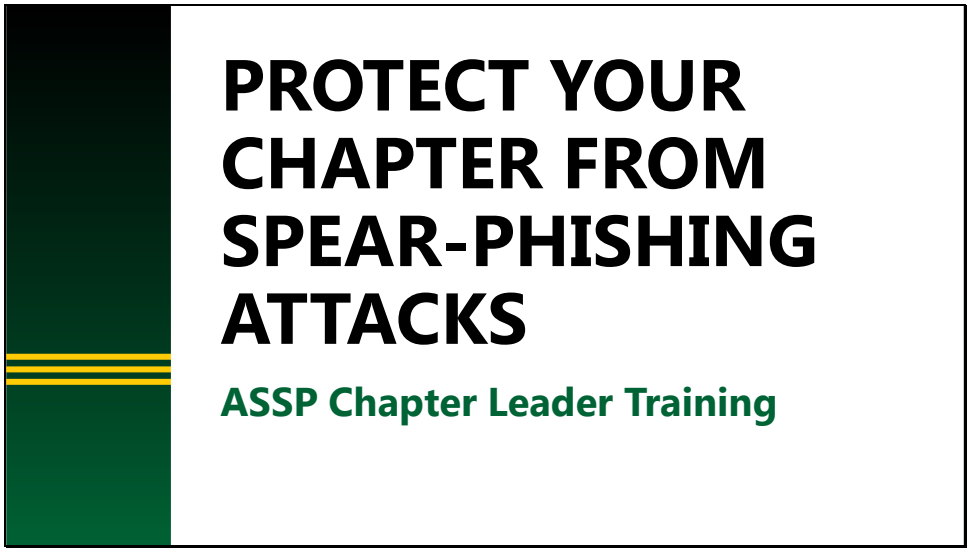


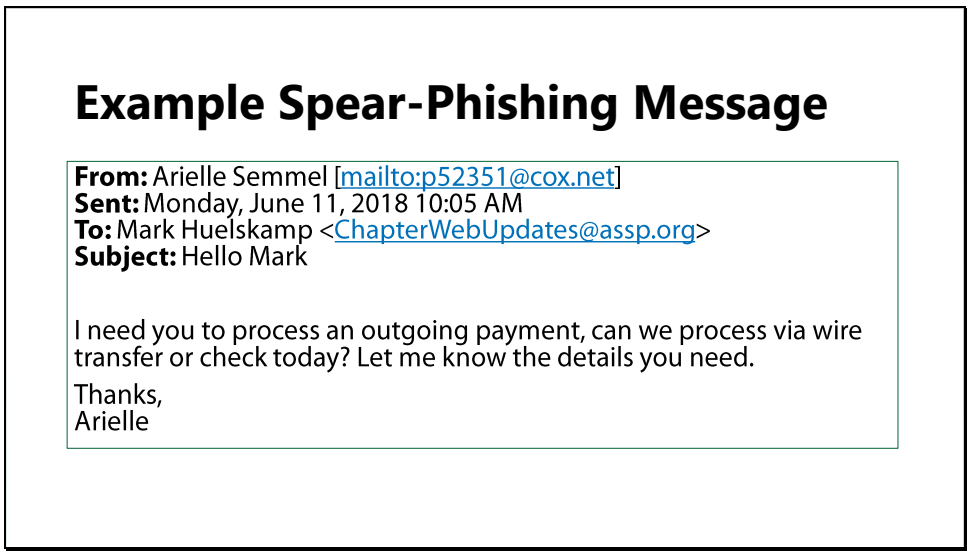
This document describes how a spear-phishing attack works, how to spot these attacks, what you can do to protect your chapter, and what you should do when your chapter is targeted.

Spear-phishing attacks are targeted email messages that come from a trusted source, likely someone the target knows personally and generally someone in a position of authority. The message content asks for a money transfer to pay a vendor or may ask for information like account and log in details.

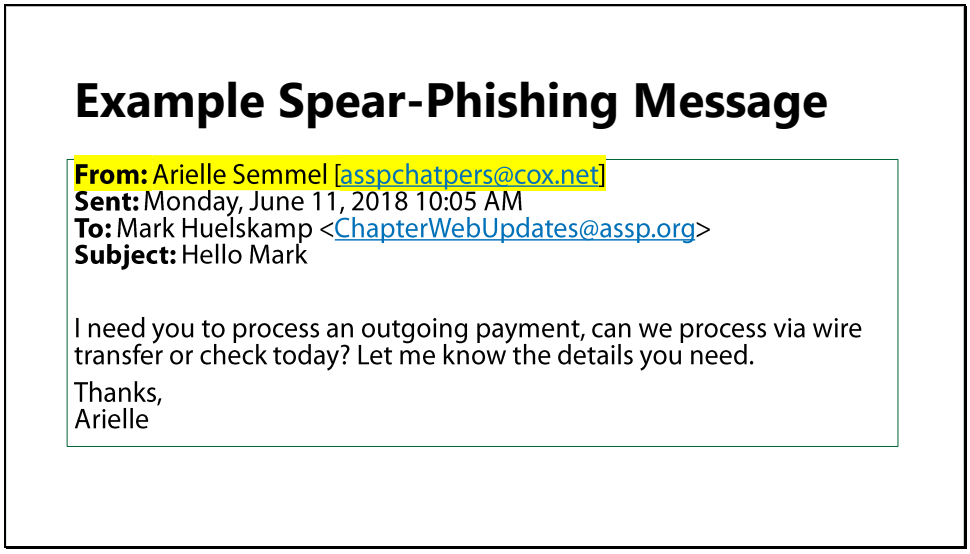
How it works: Scammers use robots to scan all types of websites across the Internet and pull the information they need for the attack. In the case of ASSP chapters, these robots are scanning your chapter website and pulling the name, position, and email contact of chapter leaders – typically the president and treasurer, though other leaders may receive messages, as well. The scammers then use this information to send their targeted messages. Being spoofed or receiving one of these messages usually does not mean your email has been hacked – it just means your information was pulled from your chapter's website.

Spear-phishing attacks and other spam messages are certainly a nuisance that comes with email communication and posting the names and contact information of your chapter leaders on your chapter's website does impact the spam in your inbox. However, your good work in keeping your website up-to-date with this information is important as you serve ASSP members – it helps your chapter members know who their local leaders are and how to get in touch with you when they want to connect.

Spam filters can block some scam messages, but spammers are increasingly finding ways around the filters. It is every email user's responsibility to be vigilant.

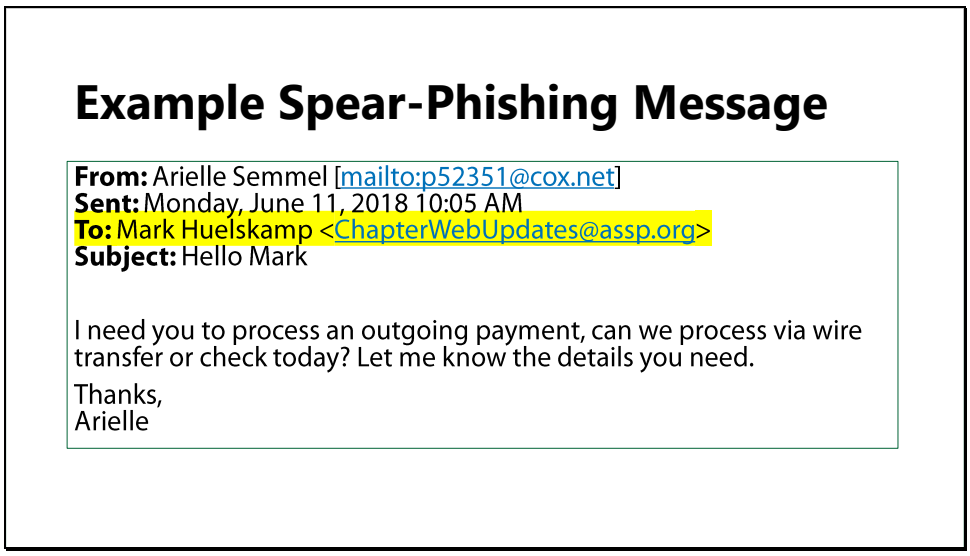


This is an example spear-phishing message based on an actual message received by one of our chapters. In this case, a scammer is posing as Arielle Semmel to target Mark Huelskamp. There are some clear ways to for Mark to tell that this message is probably spam.



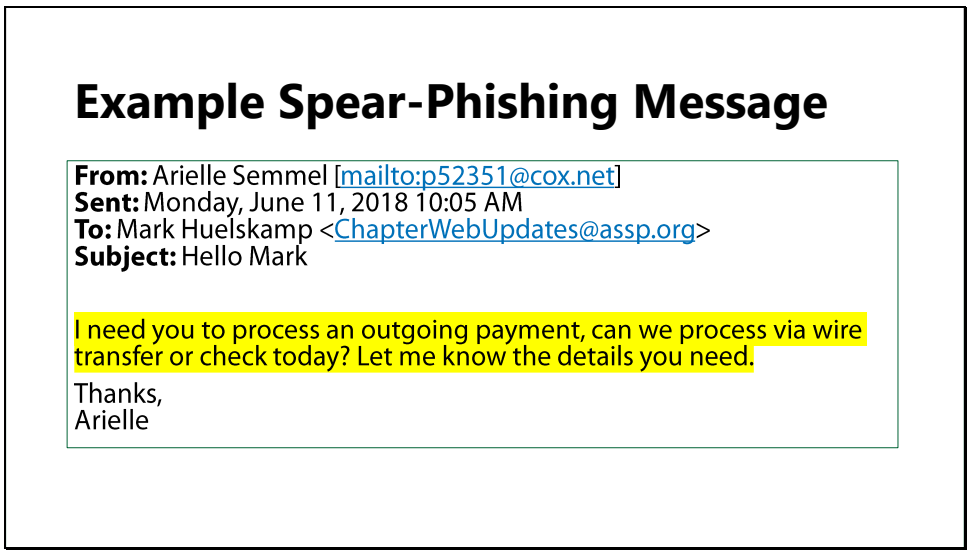
First and most obvious, Mark can check the return email address. While a spammer can spoof Arielle's name in the text field of the email, they cannot spoof an actual email address. Mark can look at the email address listed – or hit "reply" to show the email address if it does not appear. Here he can see that this is not the right email address, even though it's made to look like it could be. A closer look reveals a spelling error (chapters) and an incorrect domain name.

If Mark still isn't sure whether or not this is Arielle – perhaps she is using an alternate email address – he can pick up the phone and call her. Or, at the very least, he can send a new message to me at the email address she usually sends email messages from to ask about the request.

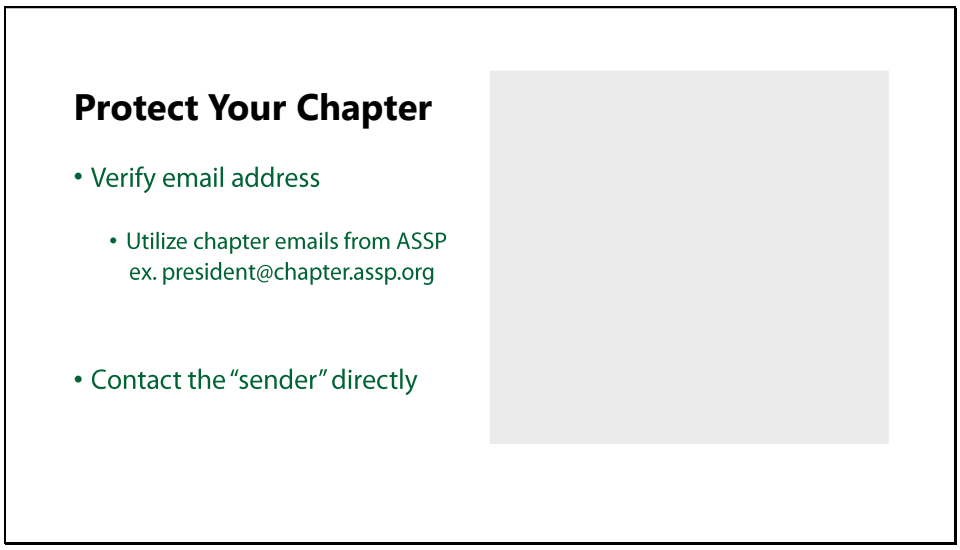


Mark can also look to see who else is included on this message. Mark and Arielle follow a best practice to include other team members that are involved on a particular project on messages – especially the messages that involve requests for payment or account information. This practice helps make sure everyone is in the loop and provides transparency to the team about what Mark and Arielle are up to.

Here, Mark can see that no one else from their team is copied on this message. Mark knows that sometimes Arielle gets busy and may miss adding the cc field, but he also knows that it's unusual for her to do that and so he knows to call to confirm the request before he sets up a payment.



Finally, Mark can take a look at the content of the message. Scammers will send vague messages that include few details about their request. Mark knows that when Arielle asks him to help with a payment, she typically includes details about who the vendor is, what exact project or event the expense is for, when the expense was approved and by who, and supporting documents like an invoice or check request form. Mark doesn't see any of that information in this message, so he knows this is a suspicious message.



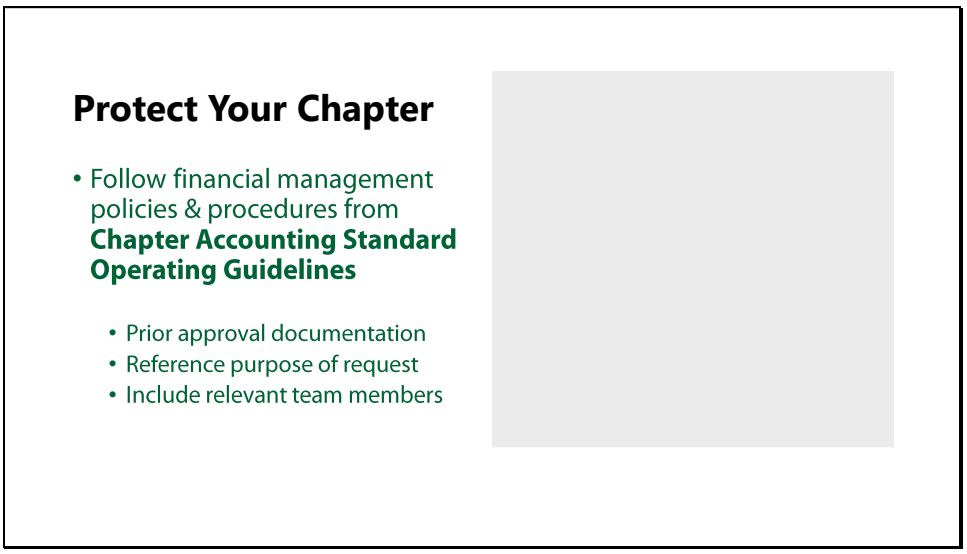
If a colleague or friend – or even a business – sends you an email asking for a money transfer, password, or other information;

- Verify the email address matches the one the sender usually uses to contact you.

You can get extra protection by utilizing role specific email addresses from ASSP. As part of the ASSP web hosting account, each chapter is offered and encouraged to use role specific email addresses for your chapter.

Again, while the plain text in the from field can be manipulated, actual email addresses cannot be spoofed. With a role specific ASSP chapter email address, you will see @[your chapter's name].assp.org in the email address when you click reply. Using chapter emails will also protect your personal information and help during the officer transition each year.

- Call or send a separate email to the person to verify if it was really that person who contacted you. The same goes for banks and businesses. Legitimate correspondence won't email you asking for same day payment, passwords, or account numbers. If you think the email might be real, call the person or company and ask.



Finally, you should always verify that any request for payment or information follows the financial management policies and requirements at your chapter, as outlined in the Chapter Accounting Standard Operating Guidelines. The Chapter Accounting Standard Operating Guidelines aim to help chapters ensure that assets are safeguarded; that financial statements align with generally accepted accounting principles; and that finances are managed with responsible stewardship.

As a chapter leadership team, have a discussion about how you will operationalize these guidelines – particularly as it relates to your email communications.

There are several practices listed in the guidelines that will help you spot and evade spear-phishing attacks.

All disbursements of chapter monies must be pre-approved by a quorum of the executive committee. In addition, any contract that will exceed $1,500 over the course of the year must be approved by both your chapter's executive committee and your regional vice president. This approval must be documented, for example, in meeting minutes. The purpose of the payment – for example, a meeting venue deposit – and the approval of those funds should be referred to in any related check requests. If you receive a request for payment that you don't ever remember discussing as a team and that does not reference prior approval, you should be suspicious.

In addition, include relevant team members in funding discussions, whether in-person or by email. While your chapter's treasurer may take the lead in financial matters, every member of the executive committee has a fiduciary responsibility to manage the chapter's finances well. Including team members in funding discussions and requests ensures that everyone is participating and is transparent in their actions and keeps everyone informed about chapter business. It also helps you question payment or information requests that don't include key stakeholders, as is usually the case in spear-phishing attacks.

What to do...

When you get the email:

- Delete the message
- Report the email address to the email service provider

If you did send payment:

- Inform your leadership team
- Report the fraud to the authorities
- Report the incident to your financial institution
- Report incident to your Area Director, Regional Vice President, and ASSP Chapter Services

If you do receive a spear-phishing email, your best course of action, as with all spam messages, is to ignore and delete the email. You can also report the email address to the email service provider so they can take the appropriate action following their usage protocols. Do not respond to the message – either to ask them to stop sending the messages or to try to trick them into giving away their true identity. This confirms for the scammers that they have a live person on the other end and will likely result in them increasing their efforts.

If you find that your chapter has been tricked by the scam and sent payment:

- Inform your leadership team. This will help them keep an eye out for similar messages – they should expect to see an increase. It will also help kick start the conversation about how your chapter wants to review its procedures and policies to prevent falling victim to any future attacks.
- Report the fraud to the authorities. While it is rare for authorities to be able to recover funds lost through email scams, it is helpful to have a police report on file for future financial audits.
- You may also want to report the incident to your financial institution, which can help you if the scammers try to access your account.
- You should also report the incident to your Area Director, Regional Vice President, and ASSP Chapter Services to help you look at ways to protect your chapter in the future. In addition, once a scammer is successful at one ASSP site, they will likely target more – sharing your experience enables ASSP to warn other chapters to be on the look-out for an increase in these messages and to take extra precautions.