CALIFORNIA NATIVE PLANT SOCIETY

Revised 1/2017

Phishing FAQs & Internet Security Guidelines for CNPS Chapters

Anyone and any business can be the target of an internet phishing scam, but if you know the warning signs and how to deal with a potential scam, you can decrease your chances of becoming a victim. CNPS staff have put together this quick guide to help you keep your chapter (and personal!) information and finances safe.

What is Phishing?
Phishing attacks use e-mail or malicious websites (that are accessed by clicking on a misleading link) to collect personal and financial information, or infect your computer or device with malware and viruses.

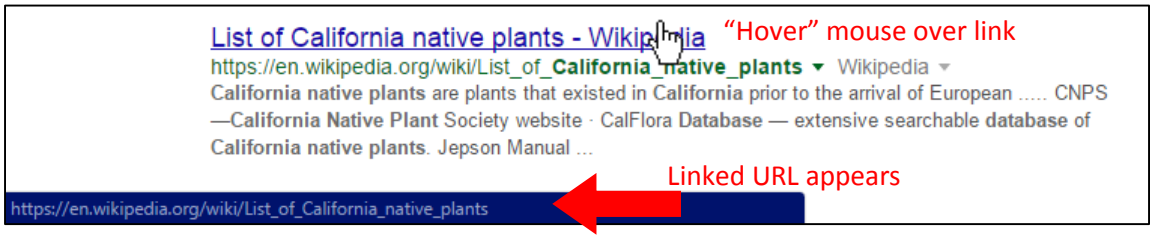
Spear Phishing
Spear phishing is a highly specialized attack against a specific target (such as a person or business), or small group of targets, designed to collect information or gain access to certain computer systems.

For example, a cybercriminal may launch a spear phishing attack against a business to gain credentials which would allow them to access customer information. They may then launch a phishing attack against these customers using the business's own internal systems, such as e-mail addresses. Fake e-mails may thus appear to be authentic, and since the recipient is already a customer of the business, the fake e-mails may more easily pass through spam filters, so the recipients may be more likely to open the e-mails and be subject to the phishing scam.

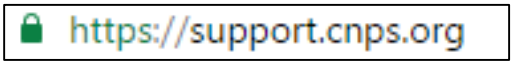
Spam & Phishing on Social Networks
Spam, phishing, and other scams aren't limited to just e-mail. They're also prevalent on social networking sites. *When in doubt, throw it out.* This rule applies to links in online ads, status updates, and other posts.

How to Avoid Phishing Scams

- Be suspicious of any e-mail or communication (including text messages, social media posts, ads, etc.) with urgent requests for personal financial information.
- Set up protections within chapter leadership. For example, set a rule that funds transfers can only be arranged over the phone or by a signed "request for funds" form, or require authorization from multiple people.
- Avoid clicking on links. Instead, go to the website by typing the web address directly into your browser, or by searching for the website in a search engine. Calling the company to verify its legitimacy is also an option. Pay attention to the website you are being directed to and hover over links (move your cursor over the link without clicking; this will show the URL that the link will send you to – see example below) before clicking. For example, an e-mail that appears to be from PayPal (https://www.paypal.com) could actually direct you to a website such as "http://www.2paypal.com" or "hxxp://www.gotyouscammed.com/paypal/login.htm" which is really a phishing scam.



- Never send personal financial information via e-mail, and avoid filling out forms in e-mail that ask for your information.
- Watch out for e-mails that seem to come from an address with a different "Reply-To" address.
- Use a secure website (i.e., URLs that begin with "https://" instead of "http://" and include a security lock icon in the address bar) when submitting credit card or other sensitive information online. Never use public, unsecured WiFi for banking, shopping, or entering personal information online, even if the website is secure. When in doubt, your 3/4G or LTE connection through your cell phone is always safer than using public WiFi.



A URL preceded by "https" and a lock icon is a secure website.

How to Deal with Phishing Scams

- Delete e-mail and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via e-mail or text.
- The messages may appear to be from organizations you do business with, such as banks. They might threaten to close your account or take other action if you don't respond.
- Don't reply, and don't click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.
- If you're wary of an e-mail but want to verify before deleting it, call a number that you're otherwise familiar with: if the e-mail seems to have come from your bank, call them at the number on your bank statement. If the e-mail seems to have come from someone within CNPS, call them by the number listed in the directory.

What Should You Do if You Think You are a Victim?

- *Report any CNPS-related phishing to the CNPS main office admin team so we can track patterns.*
- *If you believe your chapter financial account(s) may be compromised, contact the CNPS admin team immediately so steps can be taken to secure or close the account(s) as necessary.*
- If you receive a scam e-mail and would like to report it to the FBI, fill out the IC3 form here: https://www.ic3.gov/complaint/default.aspx/
- Report phishing attempts to your network administrators. They can be on the alert for any suspicious or unusual activity.
- Watch for any unauthorized charges to your account.
- Visit the FTC's Identity Theft website. Victims of phishing could become victims of identity theft, but there are steps you can take to minimize your risk.

Examples of Phishing Messages:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."
- "Please arrange for an immediate transfer of funds."

In these examples, the senders are phishing for your information so they can use it to commit fraud.