Avoiding Wildfire-Related Scams

January 23, 2025

In the wake of wildfires devastating Los Angeles County, criminals have begun targeting both victims of the fire as well as individuals seeking to help the victims. Caltech urges members of the community to be wary of any potential scams as they help one another work to rebuild their communities.

Phishing

Phishing is the use of fraudulent messages to trick people into sharing sensitive information, such as account credentials or banking information. These often take the form of someone sending a text or phone call in which they claim to be a representative from your financial institution and asking you to confirm your account number, PIN, date of birth, and other Personally Identifiable Information (PII). Once you provide them with this information, they will use it to access your accounts.

Another form they take is an email that appears to have come from a company you have an account with, for example, PayPal. The email may claim you have been logged out of your account for security reasons and ask you to visit a link to log back in. The aim is either to get you to provide your login information, or to visit a site that will install malware on your computer.

Tips to avoid Phishing:

- Enable multi-factor authentication (MFA) for email and user accounts wherever possible.
- Do not click on links contained in any email or text related to the Southern
- California wildfires. Instead, manually visit the organization's website.
- Watch out for misspelled URLs or unusual domain extensions.
- Ensure the website you are visiting is secure by looking for "https" and a padlock symbol next to the address bar.
- Do not give personal or financial information to anyone who contacts you.
- Never make a charity donation using cash
- If it seems suspicious, it probably is.

Please report any California wildfire-themed phishing emails and/or smishing texts by emailing us at calcsic_watch@caloes.ca.gov. For more information, review this announcement by the California Office of Emergency Services.

Traditional Scams

Unscrupulous individuals have begun taking advantage of both victims of the fires and those who want to help them. They may do this by pretending to represent a charity raising

money for victims. To verify that a charitable organization is legitimate, use online research resources like Charity Navigator and the Better Business Bureau. Do not give cash or banking information to anyone claiming to be from a charity without verifying their identity and their organization first.

Price Gouging

California law generally prohibits raising prices by more than 10 percent in the wake of a state or local declaration of emergency. For items a seller only began selling after an emergency declaration, the law generally prohibits charging a price that exceeds the seller's cost of the item by more than 50 percent.

This law applies to those who sell food, emergency supplies, medical supplies, building materials, and gasoline. The law also applies to repair or reconstruction services, emergency cleanup services, transportation, freight and storage services, hotel accommodations, and rental housing. Exceptions to this prohibition exist if, for example, the price of labor, goods, or materials has increased for the business.

Californians who believe they have been the victim of price gouging should report it to their local authorities or to the Attorney General at oag.ca.gov/report. To view a list of all price gouging restrictions currently in effect as a result of proclamations by the governor, please see here. For more information, please see this announcement by the California attorney general on price gouging.

As always, we ask for your help in making the campus as safe as possible. Please contact Security, at 626-395-5000 (x5000) to report any suspicious activity. Do not confront anyone on campus; instead, call Security immediately. Your safety is our primary concern. Items can be replaced, so DO NOT attempt to contact or confront anyone you suspect is engaging in suspicious or criminal activity.

###