CYBERSECURITY ADVISORY

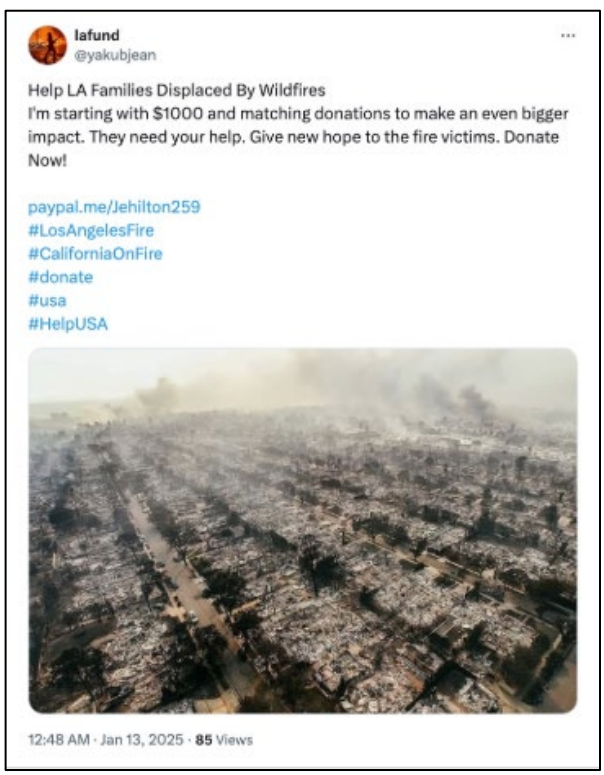
15 January 2025

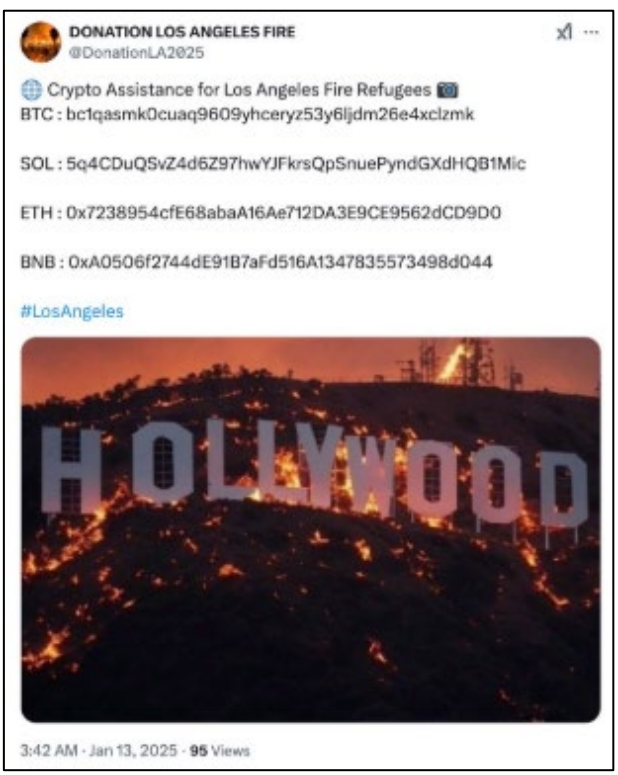
Southern California Wildfire-Themed Scams

Cyber criminals are currently exploiting the ongoing Southern California wildfires by using Southern California wildfire-themed lures for their phishing attempts and scams. Phishing is a type of social engineering attack that uses fraudulent messages to trick people into sharing sensitive information[1], such as account credentials or banking information. Phishing can be conducted through emails, text messages, QR codes, phone calls, and voicemails. Threat actors move quickly to incorporate current event-based themes into the subject matter of their phishing emails, smishing text messages, and even crowdfunding or fundraising campaign scams on social media.

Current Scams

The following are screen shots of some examples of active scams circulating social media and using the Southern California Wildfires as a lure:[2]





Best Practices

- 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.
- Watchout for misspelled URLs or unusual domain extensions. Anything other than ".com", ".net", ".org", or ".gov" would be suspicious and likely malicious.
- 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 you haven't verified.
- Never make a charity donation using cash.
- If it seems suspicious, it probably is.

Useful Contact Information

The following is a verified list of some City, County, State, and Federal agencies, and organizations you can use to verify the authenticity of any of the above-mentioned situations:[3]

Los Angeles Police Department (LAPD) • Phone: (877) 275-5373 • Website: www.lapdonline.org	California Department of Insurance • Phone: (800) 927-4357 • Website: www.insurance.ca.gov
California Contractors State License Board (CSLB) • Phone: (800) 321-CSLB (2752) • Website: www.cslb.ca.gov	Los Angeles County Consumer & Business Affairs • Phone: (800) 593-8222 • Website: www.dcba.lacounty.gov
Federal Emergency Management Agency (FEMA) • Phone: (800) 621-3362 • Website: www.fema.gov	Better Business Bureau (BBB) • Phone: (213) 631-3600 • Website: www.bbb.org

Amplifying a community alert from the Los Angeles Police Department (LAPD), the following is a list of common scams and some of their warning signs:[45]

- **Phone (Vishing) and Text (Smishing) Scams**
  Scammers may pose as FEMA, charities, or insurance agents, asking for donations or sensitive information. Hang up and verify claims directly with the agency or organization, using the contact information on their website. Avoid clicking on links or responding to unknown texts offering "help"—these are likely smishing attempts.
- **Malicious Quick Response (QR) Codes**
  Scammers often take advantage of the chaotic nature of natural disasters by creating malicious QR codes, designed to play on saving the victim time. These scams are designed to steal personally identifiable information (PII) and banking information. Avoid using any QR code not received from a validated agency or organization.
- **Suspicious In-Person Solicitations**
  Be cautious of people offering free assistance with repairs, claims, or government aid. Ask for identification and verify with the agency before agreeing to anything.
- **Gift Card or Payment Scams**
  Scammers may ask for payment via gift cards, wire transfers, or cryptocurrency. Legitimate agencies will never request payment in these forms. Report such requests immediately to local law enforcement and FBI IC3.
- **Fraudulent Donations/Fundraising Efforts**
  Verify the legitimacy of charities before donating to wildfire relief efforts. Use trusted platforms created especially for donation efforts in support of California wildfire victims.
- **False Job Solicitation Scams**
  These scams are shared on social media and falsely claim to be from reputable agencies to steal personal information. Always verify job offers through official channels or the agency's website.
- **Fake City, County, State, or Federal Employees**
  Do not trust anyone claiming to represent government agencies without proper identification. Legitimate employees won't demand payments or pressure you into quick decisions. Verify their credentials using official contact information.

Please report any California wildfire-themed phishing emails and/or smishing texts by emailing us at **calcsic_watch@caloes.ca.gov**.