03.31.20
Alert: Common Topics of COVID-19 Scams & Potential Cyber Threats

---

During this unprecedented time, [redacted] would like to caution our trusted partners about the recent wave of scams/opportunistic cyber threats taking advantage of the ongoing pandemic. Attackers are employing several mechanisms to profit from this global crisis: phone calls (including robocalls), emails, text messages, fake and phishing websites, malicious ads on reputable sites, and fake apps. Be wary of any solicitation for personal and/or financial information related to COVID-19. These scams/attacks vary greatly in content and sophistication and some may even be specific to a region or town.

To help you recognize these scams/attacks, we have listed the most commonly observed topics:

- **Promises of remedies or cures for COVID-19 or free at-home testing kits**
  Note: There is currently no cure for COVID-19 or FDA-approved at-home testing kits.
- **Alleged messages from the CDC, WHO, or random medical experts offering medical advice**
  Note: The CDC & WHO will not contact you directly. Do not communicate with anyone attempting to sell medical advice.
- **Corporate emails regarding new telework policies**
  Note: Because attackers may be spoofing your company's domain, contact your manager and/or IT to verify an email's authenticity before opening it.
- **"Expediting" of checks or loans from the $2 trillion stimulus package**
  Note: Those eligible for stimulus funds will either receive a direct deposit or a check in the mail.
- **Stimulus checks in return for completing the 2020 Census questionnaire**
  Note: Eligibility for stimulus funds is not contingent on 2020 Census questionnaire completion.
- **Unsolicited online payment of fines for violating shelter-in-place orders**
  Note: Local law enforcement will clearly inform you of penalties and how to pay fines if any are assessed.
- **COVID-19 maps for fee**
  Note: Info about COVID-19 cases in your area is available at no cost from a variety of trusted sources.

**Other observed topics include:** COVID-19 related tax refunds, promises of free or inexpensive supplies and food in exchange for personal financial information, apps that claim to help protect you from COVID-19, alleged work-from-home opportunities, COVID-19 loan consolidation programs, IT scams (taking advantage of teleworkers), and wire fraud or gift card scams at work from alleged 'senior management.'

**What to do:** Simply ignoring unknown callers, messages, and emails will protect you from most threats. Close all suspicious websites that attempt to elicit personal and/or payment information. Rely on reputable online sources for purchasing supplies and personal protective equipment (PPE.) If you receive communication from someone you know but something is suspicious about the message, contact the sender using a different mode of communication to verify he/she sent the message. Stay vigilant and remain informed about the pandemic.

**Use only trusted sources** for the most accurate information about COVID-19:

- Coronavirus.gov - https://www.coronavirus.gov
- Centers for Disease Control and Prevention (CDC) - https://www.cdc.gov/coronavirus
- U.S. Food and Drug Administration (FDA) - https://www.fda.gov/emergency-preparedness-and-response/counterterrorism-and-emerging-threats/coronavirus-disease-2019-covid-19
- National Institutes of Health (NIH) - https://www.nih.gov/health-information/coronavirus\
- World Health Organization (WHO) - https://www.who.int/emergencies/diseases/novel-coronavirus-2019


For further help, contact [redacted] at: info@redacted.com 415-858-2719