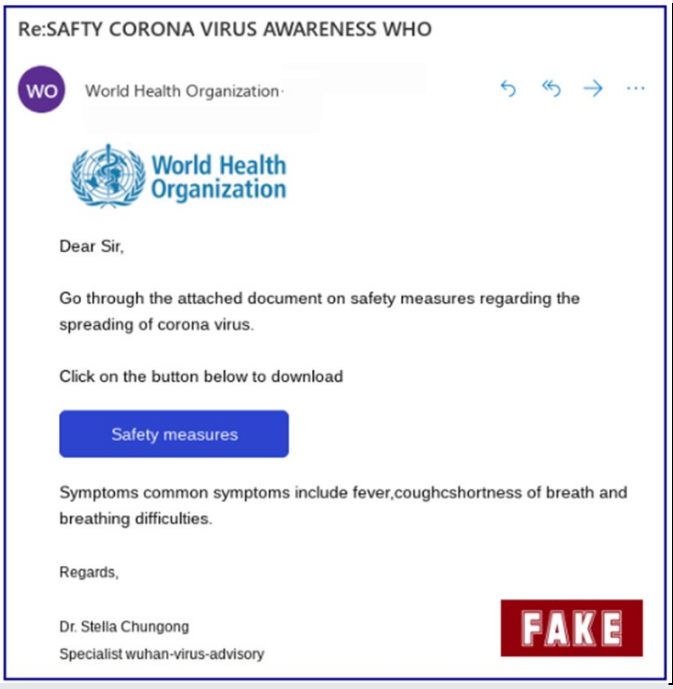
LOS ANGELES COUNTY SHERIFF'S DEPARTMENT

SPECIAL BULLETIN

SHERIFF ALEX VILLANUEVA

SITUATIONAL AWARENESS

COVID-19 Online Scams & Hacking Attempts



Warning of spike in online scams & hacking attempts related to the COVID-19 emergency

- The Fraud & Cyber Crimes Bureau, Emerging Cyber Trends Team (ECTT) has seen an UPTICK in fake emails, texts and phishing scams related to the COVID-19 emergency.
- Criminals use fake emails or texts to get you to share valuable personal information, such as: account numbers, Social Security numbers, or your login IDs and passwords.

DO NOT CLICK ON UNKNOWN LINKS, EITHER FROM YOUR CELL PHONE OR YOUR COMPUTER; INSTEAD, GO TO TRUSTED WEBSITES BY TYPING IN THE URL YOURSELF

- Trusted websites: https://covid19.lacounty.gov/ https://www.coronavirus.gov/

In light of the recent increase in online scams and hacking attempts related to the COVID-19 pandemic, the Fraud and Cyber Crimes Bureau (FCCB) - Emerging Cyber Trends Team (ECTT) is publishing this bulletin for your situational awareness.

OVERVIEW:

- Criminals use phishing emails to get access to your computer or network. **These phishing emails often appear to be from familiar company names or pretend to be someone you know.** If you click on a link, scammers/attackers can install ransomware or other programs that can lock you out of your data.
- Protect your computer and electronic devices by:
  1. Keeping your software up to date and by using security software
  2. Your cell phone should be set to update software automatically
  3. Your accounts should have multi-factor authentication
  4. Your data should be regularly backed up, and the backup should be taken offline

COMMON TACTICS:

1. **Fake charities:** When a major health event like the Coronavirus happens, you might be looking for ways to help. Some scammers use names that sound a lot like the names of real charities. This is one reason it pays to do some research before giving. When you give, pay safely by credit card never by gift card or wire transfer.

The FBI has also released the below information related to cyber enabled crimes related to the COVID-19 emergency.

2. **Fake CDC Emails:** Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize.

3. **Phishing Emails.** Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money.

4. **Counterfeit Treatments or Equipment.** Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products such as sanitizing products and Personal Protective Equipment (PPE), including N95 respirator asks, goggles, full face shields, protective gowns, and gloves. More information on unapproved or counterfeit PPE can be found at www.cdc.gov/niosh."

The following tips are the FBI's recommendations for good cyber hygiene and security measures. By remembering these tips, you can protect yourself and help stop criminal activity:

- Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall.
- Always verify the web address of legitimate websites and manually type them into your browser.
- Check for misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in .com" instead)."

Reference: FBI Public Service Announcement, Alert Number I-032020, March 20, 2020 – www.cdc.gov

ANY INFORMATION, PLEASE CONTACT

Your local Sheriff's Station or Police Department

If you prefer to provide information anonymously, you may call "Crime Stoppers" by dialing (800) 222-TIPS (8477), use your smartphone by downloading the "P3 Tips" Mobile APP on Google play or the Apple App Store or by using the website http://lacrimestoppers.org