From the desk of
Andy Siegel

What You Need to Know About COVID-19 Scams

Taking advantage of current events is a common tactic that cybercriminals use to fuel their malicious activities. With the global pandemic of COVID-19 and an overwhelming desire for the most current information, it can be difficult for users to ensure they are clicking on reliable resources. So far, the MS-ISAC has seen malicious activity come through just about every channel: email, social media, text and phone messages, and misleading or malicious websites.

The range of current malicious activity attempting to exploit COVID-19 worldwide varies. A few common examples include:

- **Fake tests or cures**. Individuals and businesses have been selling or marketing fake “cures” or “test kits” for COVID-19. These cures and test kits are unreliable, at best, and the scammers are simply taking advantage of the current pandemic to re-label products intended for other purposes. For more information on fraudulent actors and tests, check out resources from the U.S. Food and Drug Administration (FDA).
- **Illegitimate health organizations**. Cyber criminals posing as affiliates to the World Health Organization (WHO), the Centers for Disease Control and Prevention (CDC), doctor’s offices, and other health organizations will try to get you to click on a link, visit a website, open an attachment that is infected with malware, or share sensitive information. This malicious activity might originate as a notice that you have been infected, your COVID-19 test results came back, or as a news story about what is happening around the world.
- **Malicious websites.** Fake websites and applications that claim to share COVID-19 related information will actually install malware, steal your personal information, or cause other harm. In these instances, the websites and applications may claim to share news, testing results, or other resources. However, they are only seeking login credentials, bank account information, or a means to infect your devices with malware.
- **Fraudulent charities**. There has been an uptick in websites seeking donations for illegitimate or non-existent charitable organizations. Fake charity and donation websites will try to take advantage of one’s good will. Instead of donating the money to a good cause, these fake charities keep it for themselves.

Government Efforts to Reduce COVID-19 Malicious Activity

The Department of Justice (DOJ) is actively seeking to detect, investigate, and prosecute cyber threat actors associated with any wrongdoing related to COVID-19. In a memo to the U.S. Attorneys, Attorney General William Barr said, "The pandemic is dangerous enough without wrongdoers seeking to profit from public panic and this sort of conduct cannot be tolerated." Individually, most state law enforcement agencies and other judicial officials are also treating these malicious actions as a high priority. More information can be found at https://www.justice.gov/coronavirus.

Additionally, the FDA has been taking action to protect consumers from fraudulent and deceptive actors who are taking advantage of COVID-19 by marketing tests that pose risks to patient health. If you are aware of any fraudulent test kits or other suspect medical equipment for COVID-19, you can report them to the FDA by emailing FDA-COVID-19-Fraudulent-Products@fda.hhs.gov. The FDA is now aggressively monitoring and pursuing those who place the public health at risk and are holding these malicious actors accountable.

Recommendations

Exercise extreme caution in handling any email with COVID-19-related subject lines, attachments, or hyperlinks in emails, online apps, and web searches, especially unsolicited ones. Additionally, be wary of social media posts, text messages, or phone calls with similar messages.

Be vigilant, as cyber actors are very likely to adapt and evolve to the nation's situation and continue to use new methods to exploit COVID-19 worldwide. By taking the four precautions below, you can better protect yourself from these threats:

1. Avoid clicking on links and attachments in unsolicited or unusual emails, text messages, and social media posts.
2. Only utilize trusted sources, such as government websites, for accurate and fact-based information pertaining to the pandemic situation.
    - Federal Emergency Management Agency (FEMA) recommends only visiting trusted sources for information such as coronavirus.gov, or your state and local government's official websites (and associated social media accounts) for instructions and information specific to your community.
3. NEVER give out your personal information, including banking information, Social Security Number, or other personally identifiable information over the phone or email.
4. Always verify a charity's authenticity before making donations. For assistance with verification, utilize the Federal Trade Commission's (FTC) page on Charity Scams.

For More Information

If you think you're a victim of a scam or attempted fraud involving COVID-19, or you think you know of a scam or fraud, you can report it without leaving your home:

- Contact the National Center for Disaster Fraud Hotline via email at disaster@leo.gov at 866-720-5721 or the FEMA Disaster Fraud Hotline at 866-720-5721 to report frauds and scams, including personal protective equipment (PPE) hoarding or price gouging;
- Report scams and frauds to the Cybercrime Support Network ; and
- File a complaint for criminal activity by contacting your local law enforcement agency.

Additional Resources

- CDC, FEMA, and White House | COVID-19
- CDC | COVID-19-Related Phone Scams and Phishing Attacks
- CDC | Know the facts about coronavirus disease 2019
- CISA | Security Tip: Using Caution with Email Attachments
- CISA | Risk Management for Novel Coronavirus
- CISA | Information & Updates on COVID-19
- FBI | FBI Exec Discusses COVID-19-Related Schemes
- FEMA | Coronavirus Rumor Control
- U.S. DOJ | Coronavirus

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™