Centers for Disease Control and Prevention

CDC Newsroom

COVID-19-Related Phone Scams and Phishing Attacks

COVID-19-Related Phone Scams and Phishing Attacks

Phone Scams

CDC has become aware that members of the general public are receiving calls appearing to originate from CDC through caller ID, or they are receiving scammer voice mail messages saying the caller is from the Centers for Disease Control and Prevention (CDC). Some calls are requesting donations.

Downloadable apps and some free websites now make it simple for anyone to “spoof” a phone call and make it appear to come from any phone number. This is usually done by unscrupulous salespeople, in hopes that people are more likely to pick up the phone if the caller has a number similar to theirs.

Unfortunately, current technology doesn’t make it easy to block these spoofed calls, either on business or personal phones. A spoofed call does not mean that anyone’s telephone has been hacked, so you can simply hang up.

These calls are a scam and are referred to as “government impersonation fraud,” meaning criminals are impersonating government officials for nefarious purposes. Scammers are becoming more sophisticated and organized in their approach. They are technologically savvy and often target young people and the elderly.

To protect yourself from falling victim to these scams, be wary of answering phone calls from numbers you do not recognize. Federal agencies do not request donations from the general public. Do not give out your personal information, including banking information, Social Security number or other personally identifiable information over the phone or to individuals you do not know.

You can also report these calls to the Federal Communications Commission (FCC).

Phishing Attacks

Malicious cyber criminals are also attempting to leverage interest and activity in COVID-19 to launch coronavirus-themed phishing emails. These phishing emails contain links and downloads for malware that can allow them to takeover healthcare IT systems and steal information.

At least one campaign is pretending to send emails from CDC, and targets Americans and other English-speaking victims with attached notices regarding infection-prevention measures for the disease.

It is critical to stay vigilant and follow good security practices to help reduce the likelihood of falling victim to phishing attacks.

- Don’t open unsolicited email from people you don’t know.

- Be wary of third-party sources spreading information about COVID-19. Refer to the official CDC gov website for updates on COVID-19.
- Hover your mouse over links to see where they lead.
- Do not click links in emails. If you think the address is correct, retype it in a browser window.
- Be wary of attachments in any email.
- Do not supply any personal information, especially passwords, to anyone via email.

Additional resources:

- Department of Homeland Security Cybersecurity & Infrastructure Security Agency (DHS CISA)
- Federal Trade Commission (FTC) COVID-19 scams
- Department of Justice (DOJ)

Page last reviewed: April 3, 2020