[](https://now.ohsu.edu/member/post/scams-related-covid-19-rise/a540026b-9609-423c-a6a6-d7381bc454ff)

**Scams related to COVID-19 are on the rise**

Cybercriminals exploit fear to steal money and sensitive information

Scams related to COVID-19 have been increasing in recent weeks, as the world works to contain the pandemic. Scams can come in the form of emails, websites, phone calls, text messages and even fax messages.

Cybercriminals are casting a wide net with COVID-19-related phishing attempts, claiming to be:

* From Medicare, offering a health kit.
* From the Centers for Disease Control and Prevention (CDC), offering a vaccine kit. Remember: There’s not yet a vaccine for COVID-19.
* From the World Health Organization (WHO), asking for direct donations to support relief efforts.
* From the Social Security Administration, telling you there’s a problem with your Social Security number.
* From tech support, utility companies or your bank. Some are promising that you can get a lower interest rate on credit card debt, refinance your mortgage or get student loan debt forgiveness — for a fee, of course.

Get familiar with the wide variety of COVID-19-related phishing attempts being reported worldwide, so that you can better prepare yourself against them. Here are a few specific examples of recent phishing attempts and scams.

**Fake relief payments from the government**

Cybercriminals are trying to capitalize on news of the recently approved coronavirus relief bill. In advance of any possible payment, [the Federal Trade Commission (FTC) is reminding Americans](https://www.consumer.ftc.gov/blog/2020/03/checks-government?utm_source=govdelivery) of the following:

* These reports of checks aren't yet a reality. Anyone who tells you they can get you the money now is a scammer.
* The government will not ask you to pay anything up front to get this money. No fees. No charges. Nothing.
* The government will not call to ask for your Social Security number, bank account or credit card number. Anyone who does is a scammer.

**Malicious coronavirus map apps**

Malicious software ("malware") is being disguised as coronavirus maps. These apps look very convincing, but they contain malware that can steal usernames, passwords, credit card numbers and other sensitive information.

Instead of downloading an app to view the global impact of COVID-19, go directly to reputable sources, such as [Johns Hopkins University](https://coronavirus.jhu.edu/map.html). Its interactive map is accessible from any browser and does not require you to download anything.

**Thank you gifts with malicious USB drives**

The FBI is warning that cybercriminals are sending malicious USB drives to employees in the health care industry via USPS, UPS and FedEx. These USB drives come with thank you notes or other gifts — for example, you might receive a $25 Amazon gift card and handwritten note stating, "Thank you for being on the front line... enjoy this special message from our CEO!" and a USB. After plugging in the USB drive, it automatically infects the computer with malware.

**Fraudulent medical equipment sales**

The FBI is warning the health care industry in particular of an increased potential for fraudulent activity dealing with the purchase of COVID-19-related medical equipment. Based on the current stress on the supply chain, scammers may promise equipment they do not have access to in order to capitalize on the medical community’s urgent needs. The FBI asks the medical community to exercise due diligence and appropriate caution when dealing with any vendors with whom they have never worked and/or of which they’ve never heard, and when relying on unidentified third-party brokers in the supply chain.

**Learn more**

* From the WHO: [Beware of criminals pretending to be WHO](https://www.who.int/about/communications/cyber-security)
* From the FTC: [Coronavirus scams: What the FTC is doing](https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing)
* From the FBI: [FBI Urges Vigilance During COVID-19 Pandemic](https://www.fbi.gov/coronavirus)