March 11, 2020

Greetings Campus Community,

Ongoing phishing campaigns by scammers are using the recent coronavirus outbreak as bait in phishing attacks targeting individuals. These new phishing campaigns are using the coronavirus to get people to provide their email addresses, personal information and passwords. At first glance, they look like official emails, but if you look closely, you'll see it's a scam.

Coronavirus Scare Used For Phishing Scams

In one phishing campaign, the attackers promise to provide a list of active infections in the surrounding area to trick their potential victims into clicking a link embedded in the message and leading to a credential phishing page.

In another phishing email, the attackers try to pass their spam as an official alert message distributed via the Centers for Disease Control and Prevention (CDC).

Another series of phishing emails ask the recipients to "go through the attached document on safety measures regarding the spreading of coronavirus."

Coronavirus scams have taken many forms, including:

- Notices from health organizations (e.g., the CDC or local/state health departments) about local diagnoses.
- Updates from an employer about policies or procedures to address the risk.
- Information about protecting yourself, your children, or your community.
- Charitable appeals to help victims of the virus.

Here are some tips to help you keep the scammers at bay:

- Do not click on links from sources you don’t know. They could download viruses onto your computer or device.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying that have information about the virus. For the most up-to-date information about the coronavirus, visit the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).
- Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don’t let anyone rush you into donating. If someone wants donations in cash, by gift card or by wiring money, don’t do it.
- Be alert to “investment opportunities.” The U.S. Securities and Exchange Commission is warning people about online promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect or cure coronavirus and that the stock of these companies will dramatically increase in value as a result.

- Be advised that scammers may overcharge for health-related products or their shipping costs, so always comparison shop.

Be vigilant for coronavirus scams during the coming weeks. If you suspect a message may be a phishing scam, please report it by forwarding the email message as an attachment to reportphishing@csufresno.edu .

Sincerely,

Orlando Leon, Vice President for Information Technology and Chief Information Officer