DigiKnow
CYBER SECURITY DEPENDS ON YOU

COVID VACCINATION SCAMS

March 2021 | Issue 2021:2

CSO's Message

In this issue, we explore how to avoid COVID-19-related scams. Not only are scammers after your money, they're using fake vaccination sites to spread malware and steal personal information.

The bad guys produce sophisticated websites that nearly replicate real vaccination registration and other COVID-19 health-related sites. Sometimes only one letter separates a real and a fake URL.

World of Trust (WOT) is a browser plug-in application that combines machine learning algorithms with over 140 million website ratings and reviews from a global community of users that create a safety score for every website and app. Reputation icons are displayed next to search engine results, social media, emails, and other popular sites to help you make informed decisions online. A red reputation icon indicates potential danger, an orange reputation icon indicates that you need to be careful and a green reputation icon means a website is safe.

Solomon Adote
Chief Security Officer

CYBER VAX FRAUD

THREATS CONTINUE TO GROW

As soon as COVID-19 vaccines rolled out, so did the scam artists. The Better Business Bureau is getting reports of cons ranging from calls phishing for personal information, to phony messages claiming you need to pay to guarantee your dose. If you are eligible to receive the vaccine, be sure to double check any messages before sharing personal information.

A trio of Maryland men have been charged by the Justice Department for developing a phony website for COVID vaccinations, where they'd allegedly been attempting to sell the shots for $30 a pop. Authorities said the three men created a fake site made to look like the real one for Moderna Inc., with the domain name "modernatx.shop." The actual website for the Massachusetts-based company, meanwhile, is modernatx.com.

The CDC reports that 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.

CDC tips:

- 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.

For more tips and information:

Protect Yourself AVOID COVID-19 Vaccine Scams (hhs.gov)

READ MORE CYBERSECURITY NEWS at DIGIKNOW!