National Mortgage News

Coronavirus scams to watch out for

By Penny Crosman

March 11, 2020, 3:24 p.m. EDT

Fraudsters of all stripes are taking advantage of the coronavirus scare, and some of their scams are a direct threat to banks and their customers.

Granted, New York hardware stores charging $79.99 for a bottle of hand sanitizer get the spotlight. But there also hackers in the shadows sending emails and creating websites designed to trick people into clicking on malicious links disguised as helpful resources. Consumers can end up with malware on their computers that steal online banking credentials or credit card numbers.

“Cybercriminals will often take advantage of trending topics in the news, such as the coronavirus, to try and prey on consumers using fear and urgency tactics,” said Gary McAlum, senior vice president and chief security officer for USAA.

In the case of the COVID-19 pandemic, such activity is especially insidious in that it mimics communications from expert sources such as the World Health Organization, the Centers for Disease Control and Prevention and Johns Hopkins University.

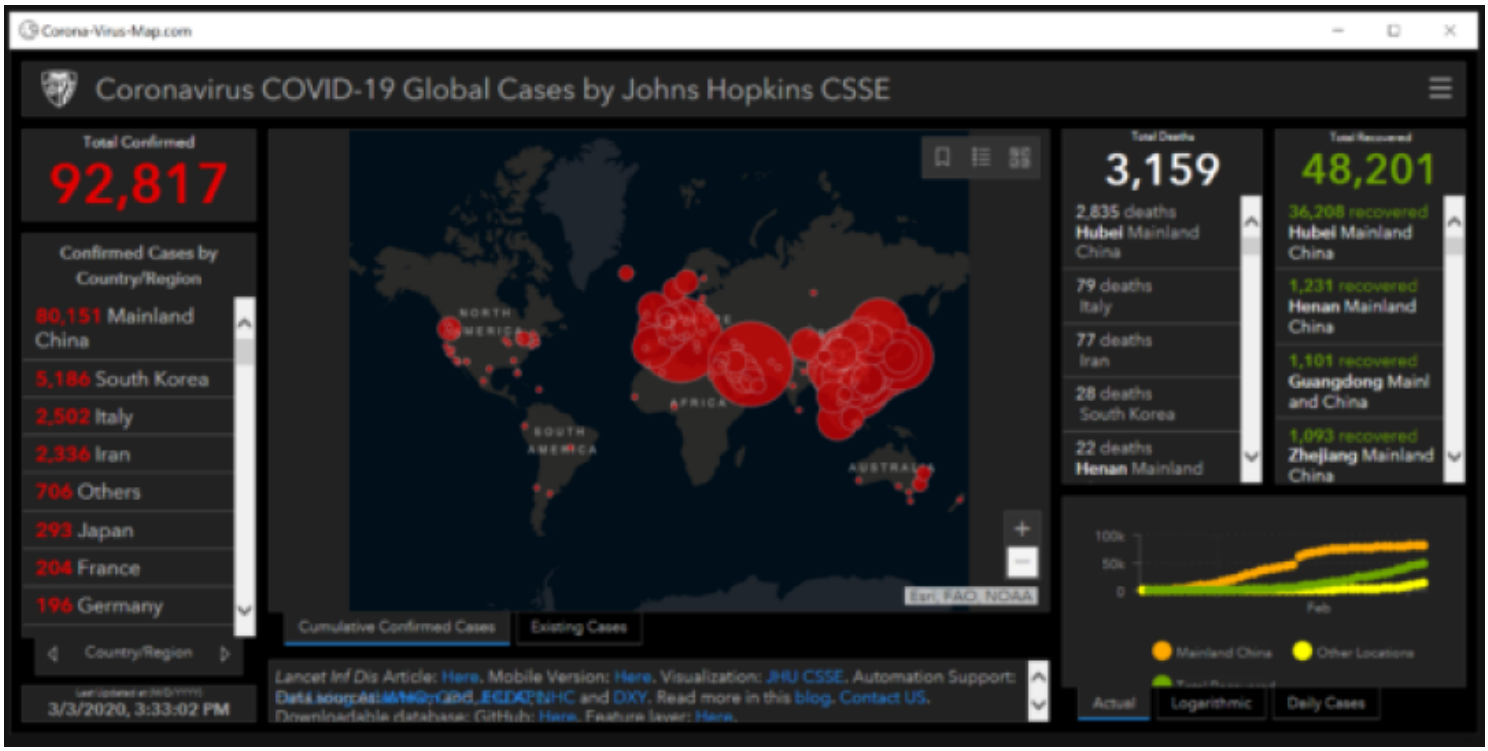
“I think false information is becoming more of a problem, especially in times of crisis, because ... everyone's looking for the best information, and they have no way of judging if it's real or not,” said Avivah Litan, vice president at Gartner. And even for consumers who consider themselves savvy enough to spot fakes, "they're not clearheaded, and they're usually very anxious to get the information, so they’re not going to analyze the URL or details of a map, images or instructions.”

These are some of the scams banks should look out for and warn employees and customers about.

The fake map

Litan's point about analyzing URLs carefully before clicking on them applies to a fake-map scam.

Johns Hopkins' popular COVID-19 dashboard has been a go-to source for people who want to stay up to date on the virus.



This fake coronavirus-related map contains a type of spyware that steals usernames, passwords, credit card numbers and other data stored in browsers.

But researchers at Malwarebytes discovered a malicious program, Corona-Virus-Map.com, that claims to provide an up-to-date coronavirus map just like the one at Johns Hopkins. It produces a map that looks exactly like the university's graphic. But the software has embedded malware called corona.exe that's a variant of AzorUlt, a type of spyware that steals usernames, passwords, credit card numbers and other data stored in the user's browser.

According to PCRisk.com, the Corona-Virus-Map.com Trojan is distributed through infected email attachments, malicious online ads, social engineering and software vulnerabilities.

Phishing

As usual, fraudsters are finding the simplest way to break into computers is through phishing email attacks.

“Phishing scams are ever-present and pervasive,” said Steven Silberstein, CEO of the Financial Services Information Sharing and Analysis Center. “Phishers are always looking for topical subjects that will capture a victim's attention. Nontargeted phishing campaigns using COVID-19 as a lure in the subject line have been observed since January. These cover the range of pre-existing threats out there, including information-stealing malware.”

Aviram Jenik, CEO of Beyond Security, pointed out that the coronavirus outbreak creates an ideal environment for phishing attacks to succeed.

“Phishing attacks are successful when one of two things happen,” he said. “No. 1, if you're flooded with information about something, it's really easy for the phishing to kind of blend in. No. 2 is, if you're uncertain, if you're getting emails about stuff and there's no concrete information, things are not really clear, you'll try to find out more.”

These phishing emails typically use the virus as a lure in the subject line; the text tries to claim news about the infections or the virus itself. Some emails claim to be from the CDC or WHO. Some offer a link to coronavirus map of the recipient’s neighborhood, or an update on how many people have been infected.

The trouble they cause runs a gamut.

“Phishing is an entry point for a variety of exploits, including stealing identities or money and delivering malware onto a victim's computer,” Silberstein said. “We have observed information stealers, banking Trojans, ransomware and remote access Trojans.”

Telling the difference between real and phishing emails is not easy.

“It's a cat-and-mouse game,” Jenik said. “It's getting harder and harder.”

One rule of thumb is that if an email asks the recipient to click on a link or go somewhere, they should always try to find another way to validate it, he said.

“If you're getting an email from your company, reach out to them on Hangouts, on Slack, or call somebody and say, is this true, is this happening?” he said. “Just try to find another channel. Don't reply to the email because you might be replying to your attacker.”

What to do

Silberstein recommended that banks continue to do anti-phishing training and use email filtering services and multifactor authentication.

“The public should not click on the unknown, especially not password reset requests,” he said. “They should use MFA for all personal email and banking accounts.”

McAlum also suggested using the strongest authentication options available, as well as account monitoring. Customers should be encouraged to set up alerts and notify their bank if they see any suspicious activity.

“They should be wary of charity scams out there,” McAlum said. “If they want to contribute, they should give to established organizations that have a known track record.”

Litan advised putting out alerts to customers warning them to be very careful about visiting websites.

“Be more paranoid than ever,” she said.

Penny Crosman Executive Editor, Technolog ne ı er