Androscoggin Bank

Member FDIC

Cyber Scams To Know

in the Wake of COVID-19

As we adjust to shelter-in-place orders, remote work, and continued social distancing more time is being spent digitally. This increase has not gone unnoticed by cybercriminals. Previously, we published a guide on scams related to COVID-19, which you can check out here.

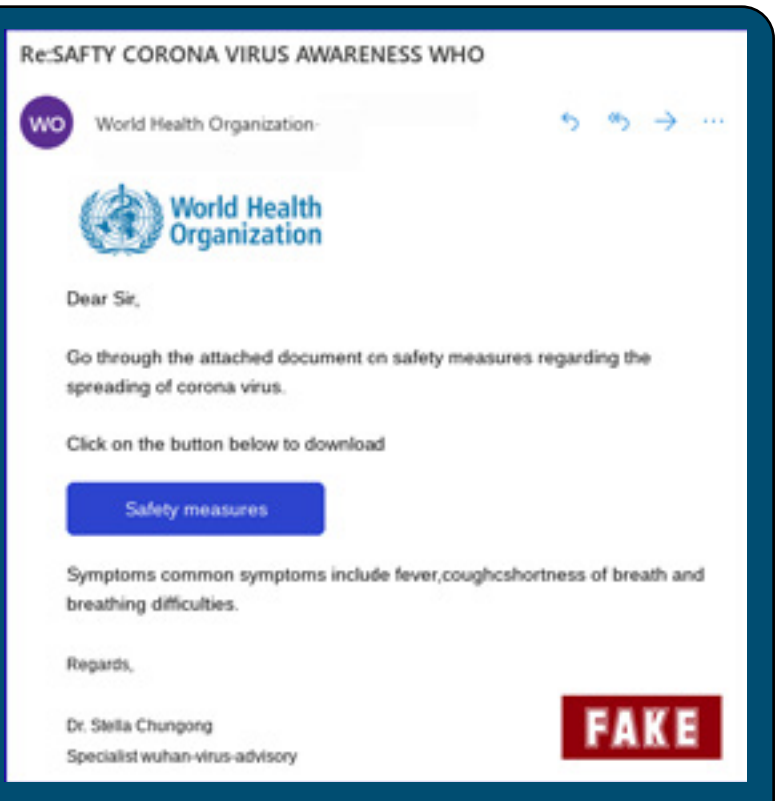
Since Our Last Guide

The FBI, the FDIC, and the Better Business Bureau have seen these attacks grow in both frequency and variety. Given the speed at which cybercriminals are ramping up their efforts to exploit the coronavirus health crisis, we wanted to provide you with the latest information on how to protect yourself.

SCAM 1

Informational/Charity

Charity scams can be tricky to identify as seen in the image to the right. These emails can come across polished and may even appear to have the support of recognized International Organizations like UNICEF. Make sure to follow cybersecurity best practices—if you need a refresher check out our original scams post here.



Informational scams tend to have a couple of key points in common making them easier to identify:
Language suggesting that the government is concealing information on a miracle cure, impact of the virus, recovery time, and so on.
The use of hair-raising language. The word “pandemic,” for example, is music to the ears of the folks behind these emails, and they are not shy about taking the term to Armageddon-levels of paranoia.

SCAM 2

Teleworkers

As organizations elect to implement telework, the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity.

Since more and more employees have switched to using their org's Virtual Protected Networks (VPNs) for teleworking, cybercriminals are increasingly focusing their attacks on VPN security flaws that will be less likely to get patched in time if work schedules are spread around the clock.

CISA also highlights the fact that malicious actors might also increase their phishing attacks to steal the user credentials of employees working from home, with orgs that haven't yet implemented multi-factor authentication (MFA) for remote access being the most exposed.

CISA has compiled a list of recommendations and direction on enterprise VPN security. Check it out here: https://go.usa.gov/xdMYJ

SCAM 3

Stimulus Check Scams

Cybercriminals are currently posing as government officials. They are sending fake texts and social media messages in attempts to siphon personal information or bank account details. The timing of these attacks is no accident as they are hoping to capitalize on public uncertainties and fears being fueled by the ongoing novel coronavirus outbreak.

The scams commonly ask you to click on a link, and then to enter personal information, including bank account records, social security number, etc. The scammers then take this information and sell it or steal your funds/identity directly.

The FBI warning to consumers and computer users from the Internet Crime Complaint Center notes, "Consumers are advised that the IRS does not initiate taxpayer communications via e-mail. In addition, the IRS does not request detailed personal information via e-mail or ask taxpayers for the pin numbers, passwords."