Androscoggin Bank

Cyber Scams To Know

in the Wake of COVID-19

For the last week news coverage has been dominated by the novel coronavirus, COVID-19. With the virus being the top of everyone's mind day in and day out, a new danger has been created—phishing attacks seeking to exploit public fears.

How Does It Work?

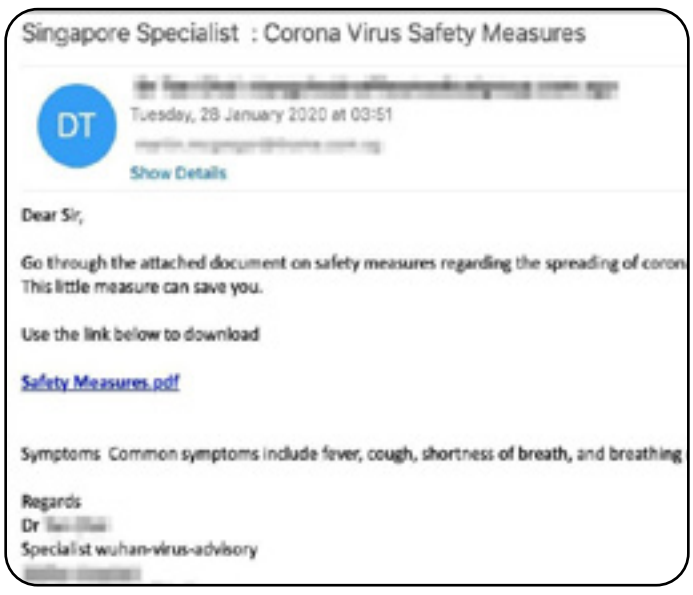
Cybercriminals send emails claiming to be from legitimate organizations with information about the coronavirus. The messages might ask you to open a link or attachment to see the latest information. In some cases, they may even ask you to donate funds for COVID-19 research or assistance. As soon as you do, your system is infected by malicious software (malware).

SCAM 1

CDC & WHO Alerts

Cybercriminals are sending phishing emails designed to look like they're from the Center for Disease Control. These emails are falsely claiming to link to a list of coronavirus cases in your area. Remember to practice the "forward slash, two dots back" trick.

Scrutinize email links by hovering your mouse over it and using the "forwardslash, two dots back" trick.
a. Go to the first forward slash after http://
b. Then count two dots back.
c. Right between these two dots is the domain the link will take you to.
d. If you do not have any valid business need to go to this link, do not click on it.



SCAM 2

Health Advice Emails

Another type of scam email claims to have advice on how to protect yourself from the coronavirus. Commonly the criminal sending the mail pretends to be a medical professional based in Wuhan, China where COVID-19 broke out.

SCAM 3

Workplace Policy Emails

The third scam growing in frequency is targeting workplace email accounts. These emails ask the user to download a policy or guideline about the outbreak, and seem to come from one's place of employment.

Protect Yourself:

The Cybersecurity and Infrastructure Security Agency (CISA) encourages individuals to remain vigilant and take the following precautions.

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.