Alert! Creative COVID-19 Scams

Clever thieves take advantage of pandemic environment

Thieves are getting creative with different ways to gain access to your checking account and personal information during the COVID-19 pandemic. Here are some of the reported schemes:

Mandatory online COVID-19 Test

Individuals posing as workers from the U.S. Department of Health and Human Services or other federal departments use text messages to instruct you to click on a link to complete a mandatory online COVID-19 test. However, there is currently no way of conducting a COVID-19 test online.

You've been in contact with COVID-19

This scam sends an e-mail to warn you that you came into contact with a colleague/friend/family member who has COVID-19. The e-mail instructs you to download and print an Excel spreadsheet and bring it to the nearest COVID-19 testing site. After opening the spreadsheet, you are told they need to enable the content in order to view the spreadsheet's details. Malicious macros are then activated when you click on the Enable Content button, infecting your computer.

SBA loan applications

Fraudulent e-mails were sent out as correspondence from the U.S. Small Business Administration telling you that you could apply for a small business disaster assistance grant. You are instructed to sign an attached document and upload it to the SBA's website. When the attachment is downloaded, a remote access trojan was installed on your computer or other electronic device.

COVID-19 malware

Online fraud and schemes wouldn't be complete without coronavirus-themed malware. There are multiple variants of a master boot record (MBR) locker, including one called coronavirus.bat. The malware replaces the MBR of a computer, preventing the operating system from starting and instead displays a ransom note or other message.

Fake pop-up testing sites

Hands down the most brazen attempt to steal personal information are pop-up COVID-19 testing sites. The thieves tell passersby that they can be tested for COVID-19 for a $240 fee. They then pocket the cash and use the personal information gathered from individuals to make fraudulent Medicare and Medicaid claims.