Coronavirus Scams

The Coronavirus has become a bonanza for scammers. Criminal hackers and scammers have been sending fake coronavirus-themed emails designed to trick people into opening attachments that download malicious software allowing access to their data. Messages have impersonated the World Health Organization and the Centers of Disease Control and Prevention. The FBI is tracking so-called phishing campaigns that seek to use people's interest in the coronavirus to get them to click on links that encourage them to reveal sensitive login information. People can report bogus emails to the FBI by going to www.ic3.gov. The World Health Organization would never ask you to login to view safety information. If a person clicks on one of the attachments promising guidance on how to "help prevent the coronavirus," malware will be downloaded onto the unsuspecting user's device. One malware package, called "Trickbot," typically tries to steal banking information and another is called "Fareit,"which can log a person's keystrokes, and tries to steal any and all login information. These few steps below can help you from becoming a victim, they include:

*Avoid opening attachments and clicking on links within emails from senders you don't recognize.

*Always independently verify that any requested information originates from a legitimate source.

*Refuse to supply login credentials or financial data in response to an email.

*Visit websites by inputting their domains manually.

The source of this information was an NBC News article entitled, "Coronavirus Scammers are Seeking to Profit off the Deadly Virus" by Ken Dilanian and Emmanuelle Saliba.