To: All ComServ Employees

From: ComServ

Date: 3-12-2020

Subject: Cyber Criminal Potential COVID 19

The purpose of this memo is to: Bring Awareness to the Potential for Increased Cyber Criminal Activity as a result of the Corona Virus.

COVID-19 is opening up opportunities for cybercriminals to further spread malicious software—specifically ransomware viruses—that are starting to infect business networks and personal computers.

Expecting that most of us will have interest in understanding the dynamics of the COVID-19 virus, hackers are devising executable files claiming to depict trackers of the virus.

Please heed caution when downloading applications related to COVID-19—specifically maps and trackers (one piece of malicious code had spoofed a Stanford University real live tracker of the virus).

Bottom line: The current pandemic and dispersion of COVID-19 merits utmost caution not only offline (to avoid contracting the disease) but also online. Cyber attackers are exploiting the popularity of coronavirus-related resources on the web, and many will likely fall prey to the attacks.

So please click wisely and seek out information from known sources such as the CDC and State of NC which are listed below.

www.cdc.gov

www.ncdhhs.gov

Thank you,

For questions, please contact Paul Norwood, pnorwood@comserve.org or Daniel Jump djump@comserve.org (828) 757 0209.