STAFF UPDATE FROM PRESIDENT PAUL CARLSEN – April 4, 2020

Team LTC,

Protecting yourself from COVID-19 extends beyond your physical health. You also need to be mindful of protecting your personal/college devices and information. Please be aware of the following malicious acts and issues occurring in the wake of the COVID-19 pandemic:

Phishing Emails: Cyber criminals have greatly increased their efforts to trick people during this global crisis. One of the biggest risks to our information security is phishing emails. These emails account for 94% of data breaches. The emails look legitimate, but typically include attachments or links to malicious websites trying to collect your login credentials or installing harmful software on your computer. As a reminder, all emails from outside of LTC will have the following banner at the top:

CAUTION: This email originated from outside of the LTC organization. Do not click links or open attachments unless you recognize the sender.

Coronavirus Maps: Most of us are familiar with online maps showing the spread of the coronavirus across the globe. Unfortunately, threat actors have put up websites with malicious maps. While these maps may have accurate data, they will install bad software, infecting your computer. The Johns Hopkins map is a favorite to copy, so be aware of that one and any others **not** located on reputable sites. The legitimate Johns Hopkins map is located here: https://coronavirus.jhu.edu/map.html.

Zoom: There has been a lot of negative press related to the communications tool Zoom. There are privacy and security concerns with how the software is built, as well as how people are using the product. LTC has not installed or endorsed using Zoom. Our primary online communication tools remain Skype for Business and Blue Jeans, so be cognizant of these concerns when calling into an external meeting using Zoom.

Thanks, Paul Carlsen