COVID-19: Cyber Security Awareness Communication

We recently became aware of instances where Cybercriminals to start taking advantage of the coronavirus epidemic. There are new Coronavirus/COVID 19 websites being created daily. Most are legitimate; however, there are hundreds being created that are identified as malicious or suspicious. Everyone must protect themselves and Trilogy and be on heightened alert before accessing websites regarding the Corona virus. **For instance, avoid such known malicious websites as those sent from @coronavirusstatus[.]space addresses.** Look for misspelled words, grammatical errors or unusual URL addresses.

If you see any emails coming from suspicious domains, or if they are links that are sent to you in emails, take extra precautions before clicking the links. If coming from an external source, do not click on any links within the email and don't open any attachments. Simply close the email and delete to avoid further risk.

There have also been reports of fake CDC links being distributed as well. If you want to access CDC information, go directly to the CDC website rather than opening via a link. The same situation has arisen with Cybercriminals creating fake websites that mirror the Johns Hopkins Coronavirus/COVID 19 transmission map. If you want to access this map, go directly to the Johns Hopkins website.