Dear Colleagues,

As COVID-19 continues to spread around the world, cyber criminals are leveraging fears of the pandemic by tailoring new phishing campaigns and other coronavirus themed scams to take advantage of those anxieties. Cyber criminals hope to prey on this anxiety and catch people off guard.

We must always remain vigilant against phishing and other similar social engineering attacks. Yet, as general anxiety around the outbreak builds, individuals may become less vigilant against certain phishing attempts and are more likely to take detrimental actions, such as providing credentials, or other sensitive information.

Known Coronavirus Scams

Attackers may send phishing emails claiming to be from the Centers for Disease Control (CDC), the Food and Drug Administration (FDA), or the World Health Organization (WHO). - *These organizations will never contact end users asking for personal information such as usernames or passwords.*

Attackers may send phishing emails claiming to be from insurance companies or healthcare organizations. These emails may convince users to login to portals, reset credentials, or divulge other sensitive information. - *As always, be vigilant when viewing, responding to, following links or opening attachments from emails containing an External Mail Banner, especially if the mail sender appears to be from someone inside of APS.*

Attackers may convince people to click on fake coronavirus statistics maps. These maps may appear to be legitimate, but they contain embedded malware, designed to steal sensitive information, including usernames and passwords. - *Anyone wishing to view COVID-19 infection statistics or maps should rely on legitimate websites for this information. The University of Minnesota has a comprehensive list of resources available at* http://www.cidrap.umn.edu/covid-19/maps-visuals

Attackers may seek to defraud users wishing to donate money by creating fake charity organizations. These fake organizations will claim to assist COVID-19 victims or response efforts. - *You should always confirm the legitimacy of any charity organization before donating.*

Attackers may prey on general anxiety by offering products to treat, prevent, or cure COVID-19 infections. - *Currently, there are no vaccines, pharmaceuticals, or other products available to treat or cure COVID-19—online or in stores.*

Legitimate Websites for update information on the COVID-19 Outbreak

U.S. Centers for Disease Control and Prevention (CDC) - http://coronavirus.gov/
Georgia Department of Public Health - https://dph.georgia.gov/novelcoronavirus
Atlanta Public Schools Covid-19 Updates - https://atlantapublicschools.us
OSHA - https://www.osha.gov/SLTC/covid-19/
The US Food and Drug Administration - https://www.fda.gov/emergency-preparedness-and-response/mcm-issues/coronavirus-disease-2019-covid-19

The World Health Organization (WHO) -https://www.who.int/emergencies/diseases/novel-coronavirus-2019
US Department of Homeland Security - https://www.dhs.gov/news/2020/03/13/fact-sheet-dhs-notice-arrival-restrictions-china-iran-and-schengen-countries-europe

If you suspect that you were a victim of a phishing scheme, please notify the APS IT Security as soon as possible at netsecure@atlanta.k12.ga.us