DigiKnow

CYBER SECURITY DEPENDS ON YOU

December 2020

A Note from Our Chief Security Officer Solomon Adote:

As 2020 comes to the end, I want to say thank you to all of the behind - the- scenes heroes that I have had the pleasure of working within state government. Our IT community has stepped up to every challenge, working long days and weekends too. The results? Virtual learning for all Delaware's K-12 students, a fully equipped remote workforce and a robust contact tracing program. All of this accomplished in a world where cyber threats and scams are more sophisticated and intrusive than ever before.

Wishing you a healthy and happy holiday season.

The Not So Jolly 2021 Cyber Threat Forecast

Cybercriminals have taken advantage of the fear and uncertainty associated with the COVID-19 pandemic. Microsoft reports that pandemic-related phishing and social engineering attacks have skyrocketed to 30,000 a day in the U.S. alone. The attacks have affected all organizations in all industries including government. Checkpoint research finds that Phishing campaigns will intensify as COVID-19 continues to impact the world. The race is on to begin the vaccination roll-out and scammers will step up their phishing campaigns too. Drug companies developing vaccines will be targets of malicious attacks orchestrated by criminals or nation-states aiming to exploit the situation.

There will be more focus on social engineering. Watch out for e-cards this holiday season. Phishers send an email message letting you know that someone has sent you an e-card. It includes a link or attachment that often appears to look like it came from a legit card company like Hallmark or 123Greetings. Clicking the link or opening the attachment can launch dangerous malware. Watch out for emails that say a "friend" or "secret admirer" has sent you a card. Another indicator is messages with misspellings or poor grammar.

In the wake of the COVID-19 lockdown, schools had to swiftly shift to e-learning environments which led to attacks on remote learning. Educational facilities were hit by a 30% increase in weekly cyberattacks during August while they prepared for the new semester. A ransomware attack in late November shut down Baltimore County schools' virtual learning for two days. These attacks may persist, disrupting remote learning activities.

Be suspicious of emails. Be wary of messages purporting to be from government agencies, especially when it comes to COVID-19 research and vaccinations. Be vigilant in keeping your devices and machine updated.

Winter Vacation Cyber Games

CyberStart America is an online set of challenges that allow students to become Cyber protection agents, solving puzzles and exploring all things Cyber-related. The program is free for all Delaware students in grades 9-12. Scholarships totaling $2 million will be awarded to 600 high-scoring students nationwide. The challenge started November 15 and closes February 28, 2021. Students can join anytime. Complete details can be found at: www.cyberstartamerica.org.

Questions, Comments, or Topic Suggestions? Email us at eSecurity@delaware.gov

Department of Technology & Information
Delivering Technology that Innovates

Delaware Department of Information & Technology publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.