RUSSIA-UKRAINE CONFLICT
What are the Cybersecurity Implications?

February 2022 | Issue 2022:2

What is DTI Doing to Protect Delaware's Data?

The situation between Russia and the Ukraine has potential for far-reaching cybersecurity concerns and issues. Currently, the U.S. government is not reporting any cyber attacks directed at our systems or infrastructure but the Department of Homeland Security (DHS) has issued a formal warning.

While there is not yet any known direct, credible, or specific threat to Delaware's critical infrastructure, DTI has alerted our state government's Information Security Officers (ISO) of actions being implemented to protect our citizens' data. We are committed to safeguarding our networks and systems.

Cybersecurity is everyone's responsibility, particularly when an attack is a real possibility. Be alert, aware, and report any unusual incidents to your organizations' ISO or Service Desk.

Solomon Adote
Chief Security Officer

Difficult Times Call for Increased Diligence
Learning About Website Categorization

Russia and Ukraine tensions are escalating, and intelligence sources anticipate increases in cyberattacks on the United States and its critical infrastructure. Offensive cyber operations are a recurring aspect of the Russia-Ukraine conflict. the Department of Homeland Security has recently warned that any United States response to a possible Russian invasion could result in cyberattacks launched against the United States by the Russian government or its proxies.

One weapon in Delaware's cyber war arsenal is Website Categorization. On the network level DTI utilizes several products that provide website categorization, assigning levels of risk in to determine the safety of users accessing them. These products can include features like geo-location, which offers the ability to create access policies based on the country location of a website.

State network users will begin to see a message appear if they are browsing and a site is "uncategorized". The message will notify them that the site is uncategorized and may be risky. If there is a business need to proceed to the site, it will be accessible, but the user needs to consider if the risk is worth continuing to the website.

To protect yourself at home against the potential for being victimized by a cyber attack, there are a number of trusted sites offering browser protection plug ins. Free protections that can be downloaded for home use include: WOT – Web of Trust and McAfee Web Advisor.

Website Safety Check & Phishing Protection | Web of Trust (mywot.com)

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

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/news/index.shtml?dc=newsletters