DigiKnow
CYBER SECURITY DEPENDS ON YOU

SEE SOMETHING, SAY SOMETHING

June 2024| Issue 2024:6

WHAT IS THE DIAC?

The Delaware Information and Analysis Center (DIAC) helps safeguard the community by serving as a dynamic security nexus. To detect, prevent, investigate, and respond to criminal and terrorist activity, DIAC disseminates intelligence and facilitates communications between state, local, federal agencies, and private sector partners, to help them take action on threats and public safety issues.

What many of us are unaware of is the role that the average Delawarean can play when it comes to the DIAC.

Report! Because the solution starts with you.

Preventing terrorist or other criminal activities and emergencies is much easier and more effective than reacting to the aftermath. And it saves lives.

This holds true when it comes to cyber threats. Cyber criminals increasingly are involved in ransomware activities. These range from data breaches and theft to threatening to release disparaging or embarrassing information about a person or organization.

That's why the DIAC encourages you to contact your local law enforcement agency with tips on wanted individuals, unsolved crimes or potential threats.

Solomon Adote
Chief Security Officer

CYBERSECURITY IS EVERYONE'S JOB

The **"See Something, Say Something"** campaign is a national initiative that encourages individuals to be vigilant and report suspicious activities that could indicate terrorism or terrorism-related crimes. In the context of cybersecurity, this means being aware of and reporting activities that may signal a cyber-attack or a security vulnerability.

Awareness: The campaign aims to raise public awareness about the signs of terrorism and how to report suspicious activity to state and local law enforcement.

Reporting: If you notice something out of the ordinary that could suggest a potential threat, you are encouraged to report it to local authorities.

Signs of Suspicious Activity: Knowing what constitutes suspicious activity, especially in the digital realm, is crucial. This could include unusual network activity, phishing attempts, or unexplained system changes.

Community Role: Everyone has a role in keeping communities safe, and this includes staying alert during daily routines and speaking up when something seems amiss.

Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices for federal law enforcement.

State Employees should report work-related incidents promptly to their Information Security Officer (ISO). ISOs are the intermediaries between a State organization and DTI when it comes to security and risk of operations. Email our **eSecurity office** to determine the ISO for your agency.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information 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

Department of Technology and Information
Contact us at **esecurity@delaware.gov**