Back to School Cyber Safety

The Delaware Information & Analysis Center (DIAC) is providing the following for informational and situational awareness. As summer break ends, many students will be returning to school with mobile devices, such as smart phones, tablets, and laptops. Although these devices can help students with their assignments and stay in touch with family and friends, there are security risks associated with using them. However, there are simple steps that can help keep students stay safe while using their mobile devices and getting online.

The National Cybersecurity and Communications Integration Center (NCCIC) recommends reviewing the following tips and resources for information on how to keep students cyber safe:

- Keeping Children Safe Online
- Rethink Cyber Safety Rules and the “Tech Talk” with Your Teens
- Building a Digital Defense for School Kids and Cell Phone Safety
- Stop, Think, Connect. Toolkit
- Stay Safe Online
- Concerned Parent’s Internet Safety Toolbox

The attached Federal Bureau of Investigation (FBI) Private Industry Notice (PIN) titled Connected Education Technology and Mass Data Collection on Student Necessitates Increased Cybersecurity, is being re-sent for situational awareness. Cyber criminals that target children can exploit education technologies (EdTech) and school data systems which house large amounts of student information. Academic organizations serving K through12 communities should be aware of the cybersecurity risks to better protect students and their data.

DIAC is always seeking information on:

- Suspicious cyber activity affecting government systems.
- Suspicious cyber activity affecting critical infrastructure systems.
- Suspicious consumption and sharing of media glorifying violent extremist acts.

To report suspicious cyber activity in Delaware to DIAC by email at DIAC@state.de.us.

Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). No portion of this document should be released to anyone outside of the intended recipients. Care should be exercised in order to protect the contents of this document and restrict its access. This printed document should be disposed of in accordance with existing OPSEC standards in the handling of FOUO materials. Even though this document does not contain classified information, it is requested that this document not be disseminated without prior approval from the Delaware Information & Analysis Center (DIAC).