ALABAMA SECURITIES COMMISSION
Post Office Box 304700, Montgomery, Alabama 36130-4700
Telephone: (334) 242-2984 or 1-800-222-1253 Fax: (334) 242-0240
Email: asc@asc.alabama.gov Website: www.asc.alabama.gov

Back-to-School Means More Time Online
Cyber Criminals Are Also Increasing Screen Time

Montgomery, Alabama (August 10, 2026) – As thousands of Alabama students prepare to head back to classrooms and college campuses, the Alabama Securities Commission (ASC) is urging students and families to make cyber safety a priority.

Most of us, including students, have constant access to the internet via phone, tablet, or computer. The smartphone has evolved to become an essential device that most of us cannot function without. Students are spending more time than ever online, attending classes or seminars virtually, conducting research, applying for scholarships and academic programs, and communicating through email, text messages, and social media. As students spend more of their academic and personal lives online, they are becoming increasingly attractive targets for cybercriminals. The FBI Internet Crime Complaint Center (IC3) received a record-high of 1,008,597 internet crime complaints during 2025. The record-breaking complaints also accounted for over $20.8 billion in losses, which was a 26% increase from 2024.

Cybercriminals target everyone, even minors. In 2025, there were 13,168 complaints involving victims ages 17 years old and younger, with the reported loss totaling nearly $13 million. The average loss was $986. Investment-related scams caused the greatest loss, accounting for more than $4.7 million in losses.

Artificial intelligence (A.I.) has significantly changed the fraud landscape. Criminals are now using A.I. to create convincing emails, text messages, fake customer service representatives, fake invoices- including tuition payment scams, cloned voices, realistic websites, and deepfake videos that can appear to be legitimate, even over video conferencing platforms. The FBI recently identified A.I. fraud as one of the fastest-growing cyber threats in the United States.

Online shopping and college tuition scams are also common during the back-to-school season. Fraudsters often advertise heavily discounted electronics, textbooks, and dorm essentials through fake websites and social media advertisements luring consumers into providing financial or personal information. Likewise, scammers may also impersonate schools and colleges, using fake websites and fraudulent invoices to claim that tuition is due or that the financial aid office needs additional documentation, including bank account information. "A.I. is a tool that many of us use to become more efficient, but cybercriminals are using A.I. for the same reason and will exploit any opportunity, including ‘back to school’, to target specific populations. They leverage A.I. to communicate with victims via email, text, audio, and video calls enabling them to impersonate friends, family, law enforcement, and businesses,” said ASC Director Amanda Senn. “Students and parents should slow down, think twice, and verify, before clicking links, sending money, or sharing personal information.”

ASC encourages students and families to follow these cybersecurity best practices:

- Verify website addresses before making purchases or entering payment information. Contact the businesses directly by using a verified phone number or conduct research online. Fake businesses often have little or no online presence, unusually high ratings or customer comments. Be cautious of websites that appear to belong to a legitimate business but are actually fraudulent replicas designed to steal personal or financial information.
- Be cautious of unsolicited emails or text messages requesting passwords, personal and financial information, or that require immediate action- especially demands for money.
- Never trust unexpected investment opportunities promoted through social media, messaging apps, or text messages.
- Enable multi-factor authentication on school, banking, and shopping accounts and use strong, unique passwords for every online account.
- Research and verify scholarship offers, internships, and online job postings before providing personal information.
- Discuss A.I. scams with family members so everyone recognizes that voices, videos, and emails can now be generated to seem real.

"If something seems too good to be true, or creates a sense of urgency, stop and verify," Senn said. "Don’t trade a few minutes of convenience for years of frustration and anxiety. An ounce of caution is worth years of peace of mind.”

The ASC cautions investors to thoroughly research any investment opportunity. Call the ASC at 1-800-222-1253 and ask the registration department to check out individuals offering investment opportunities, investment advice for a fee, and any products they offer. Contact the ASC to report suspected fraud, inappropriate securities business practices, or to obtain consumer information. Free investor education and fraud prevention materials are available at www.asc.alabama.gov.

###