

Key Actionable Insights for a Cybersecurity Student:

1. Recognize and Verify Official U.S. Government Websites: Always ensure the website you're visiting has a ".gov" domain, as it belongs to an official government organization in the United States. Also, look for a lock icon or "https://" on the address bar, which indicates that the connection is secure.
2. Use Secure Government Websites for Sensitive Information: Share sensitive information only on official, secure websites identified by the presence of "https" and a locked padlock in your web browser's address bar.
3. Utilize Free Cybersecurity Services and Tools: Leverage resources provided by the Cybersecurity and Infrastructure Security Agency (CISA), such as Free Cybersecurity Services, Secure by Design, Secure Our World, Shields Up, and Report a Cyber Issue to enhance your cybersecurity knowledge and skills.
4. Stay Updated on CISA News & Events: Regularly visit the CISA news and events page to stay informed about important communications, advisories, alerts, and upcoming events hosted or participated in by CISA.
5. Follow Emergency Directives and Binding Operational Directives (BODs): Keep yourself updated on the latest directives issued by CISA, such as ED 24-01, BOD 23-02, BOD 23-01, and BOD 22-01. Follow these directives to improve your organization's cybersecurity posture and address known exploited vulnerabilities in a timely manner.
6. Register for CISA Webinars: Sign up for webinars organized by CISA, such as Active Shooter

Preparedness Webinars, to gain valuable insights into potential threats and best practices for preparedness and response.