***A picture containing text, clock

Description automatically generated***

This project was supported by the Cybersecurity and IT Pathways grant from the Florida Department of Education through Cyber Florida, project number 291-1231C-2C001, funding authority 84.425C-D CRRSA ACT ESSER II 84.425D & GEER II 84.425C, FAIN#: S425C210052. More information at cyberflorida.org/pathways/

**Terms and Definitions**

Chapter 16 Cybersecurity

The Chapter Terms and Definitions was written for the Florida Public School System DIGITAL INFORMATION TECHNOLOGY (8207310) course. Funded by the Cyber/IT Pathways Program, Cyber Florida, and the Florida Department of Education.

# Chapter 16 Cybersecurity

| **Term** | **Definition** |
| --- | --- |
| Asset | A resource or information that is to be protected |
| Brute Force Attack | A programming script designed to repeatedly execute its code while attempting to log into a system with a user account |
| CIA Triad | The provision of confidentiality, integrity, and availability. By protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction |
| Control | Safeguards used to minimize the impact of threats |
| Cyber Hygiene | The practices which reduce the risk of a successful cyber-attack |
| Cybersecurity | Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to make sure its availability, integrity, authentication, confidentiality, and nonrepudiation |
| Denial of Service Attack | The act of more than one networked computer overwhelming a network with fraudulent traffic |
| Hacker | A person who wishes to gain access to an identified target to learn more about the target and exploiting the target for an attack |
| Information Security | Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability |
| Malicious Actor | Someone or something that causes harm in the digital domain |
| Phishing | Attempting to compromise a user by masquerading as a trustworthy entity in electronic communication |
| Social Engineering | When deception is used to make a person give up private information or provide unauthorized access to a computer system or network |
| Threat | The capabilities, intentions, and attack methods of adversaries to exploit or cause harm to assets |
| Virus | A computer program that uses other programs to spread and adversely affect computers and propagate through the network without the user’s consent |
| Vulnerability | A weakness in an information system that contributes to a threat with the opportunity to compromise an asset |
| Worm | A computer program that can propagate all by itself and adversely affect computers and propagate through the network without the user’s consent |