4.CYB.2 Cybersecurity

> *The student will identify and investigate best practices to safeguard information shared online and through online platforms. (a) Classify personal, private, and public information. (b) Research and evaluate tradeoffs of sharing information. (c) Investigate and communicate best practices to limit unauthorized access to information on a computing device. (d) Demonstrate proper use and protection of personal passwords.*

Understanding the Standard

The internet allows us to connect with others and have access to their information instantly. However, it's important to protect personally identifiable information. To protect private information, many online platforms use authentication, or making sure that only certain individuals have access to a person's information, through the use of passwords, personal identification numbers (PIN), or two-factor authentication. Because computer programs can be used to guess passwords, strong passwords have characteristics that make them more difficult to guess. Many websites have rules as to the length and composition of passwords; these rules help create stronger passwords. Students should explain how passwords help protect privacy, classify strong and weak passwords, and discover how strategies such as logging off of devices and keeping passwords a secret can help protect information.

Term	Definition
Authentication (also called authorization)	The process of identifying a person and making sure they are who they say they are, such as using a password, a PIN, or biometric information.
Password	A secret code used to log into accounts and keep information private.
Strong password	An effective password that would be difficult to break.
Weak password	A password that is easy to guess or to break by repeatedly trying a list of words or letter combinations.

Prerequisite Knowledge

Students should have a basic understanding of safe and unsafe actions and knowledge of the word "private" as applied to information.

Integration Opportunities

English 4.C.1a Conduct peer discussions of best practices for safeguarding online information. Students should summarize ideas with evidence, examples, and details that support opinions and conclusions.

Health 4.2.k, 4.3.k Have students identify personal, private, or public information that might be shared online and explain what to do if someone asks for personal information, then create a personal online safety plan.

Math 4.PS.1 As part of a campaign aimed at educating peers about digital safety, collect and analyze data on student online practices. A line graph could illustrate how students' understanding of digital safety practices changed after different stages of the campaign.

Summary of a Lesson

Introduce the class to the Password Ninja password generator (or another password generator). Have students generate and record 10 passwords and discuss how difficult it might be to guess one of the passwords. Give students the opportunity to explore the advanced features to customize passwords and make them more difficult to guess. Categorize passwords as "easy to guess," "difficult to guess," "easy to remember," and "difficult to remember," and describe the relationships between passwords in each category. Review with students characteristics of a strong password, including: uses uppercase and lowercase letters, numbers, and symbols; uses at least 8 characters; not words from a dictionary; not personal information; not reused from another site. Have students practice creating their own new password that meets all the requirements.