# 5.CYB.1 Cybersecurity

> *The student will identify ways to limit unauthorized access on computing devices. (a) Define virus, malware, and phishing. (b) Explain how viruses and malware can put personal information at risk. (c) Describe the role of human interactions in social engineering attacks. (d) Identify ways to protect personal and private information when using a computing device and the Internet. (e) Explain the importance of updating software.*

## Understanding the Standard

Technology allows people to connect, have access to information, and to share ideas. To keep students safe, schools and school divisions have rules on the appropriate use of technology. As students increase their use of technology and interaction with others outside of the school/home environment, it's important to teach students how to navigate the internet, use technology safely, and minimize the risk of having data compromised by threat actors, those who would intentionally cause harm. Understanding how deceptive techniques, such as malware and phishing, exploit human trust and interactions to gain access to secure information will help students build habits that protect their information throughout their lives. To further support these habits, it is important to establish and regularly review classroom, school and school division safety protocols.

| Term | Definition |
|---|---|
| Virus | A malicious program, script, macro, or code designed to damage, steal personal information, modify data, send email, display messages, or a combination of these actions. (from ComputerHope) |
| Malware | Software that uses deceptive and unethical tactics to install itself on a computer without consent, causing harm by potentially disabling or disrupting computers (adapted from ComputerHope) |
| Phishing | A malicious technique of tricking users into giving away personal information to an attacker. (from ComputerHope) |

## 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

**History USI.6e, USI.9f** Explore cryptography and how information was protected through codes during the Revolutionary and Civil Wars.

**English 5.RI.1 a,b** Research and summarize informational text regarding cybersecurity. Summarize the main idea and concepts including what happened, how, and why.

**Math 5.PS.3** Design a game where students determine the probability of selecting secure versus risky actions (e.g., choosing strong passwords, avoiding malware) and discuss how these choices can impact the risk of unauthorized access on a computing device.

## Summary of a Lesson

As a class, review your school/division's appropriate use of technology policy. Break students into groups (3-4 students). Each group is provided with a scenario that could happen when using the Internet (e.g., a student receives an email with a link that they weren't expecting, a social media challenge suggests sharing important dates). Students work with their group to identify which aspect of the technology policy (if any) was broken, possible consequences/dangers of this scenario, and an appropriate response to if they were to witness the scenario. Students will then work as a group to create a 1-3 minute skit or 1-3 slide presentation that will summarize the scenario, identify the rule broken, the appropriate response and possible effects of the scenario. As a class, evaluate the existing technology policy and suggest revisions to help the policy better support student activities.