<table>
<tr><td>Time Frame: 3 weeks</td><td>Unit Title: Cybersecurity</td><td>Course Name: Technology and Society</td></tr>
<tr><td colspan="3">Stage 1 - Desired Results</td></tr>
<tr><td rowspan="8">Established Goals

NH Computer Science Standards

IC – Impacts of Computing

2-IC-23 - Describe tradeoffs between allowing information to be public and keeping information private and secure.

3A-IC-29 - Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.

3A-IC-30 - Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.

3B-IC-28 - Debate laws and regulations that impact</td><td colspan="2">Transfer</td></tr>
<tr><td colspan="2">Students will be able to independently use their learning to…

Protect personal data when using computing innovations in an increasingly digital world.</td></tr>
<tr><td colspan="2">Meaning</td></tr>
<tr><td>UNDERSTANDINGS
Students will understand that….

The use of computing innovations may involve risks to personal safety and identity.</td><td>ESSENTIAL QUESTIONS
Students will keep considering

How is cybersecurity impacting the ever-increasing number of Internet users?

Should individuals allow private companies access to their digital data?</td></tr>
<tr><td colspan="2">Acquisition</td></tr>
<tr><td>Students will know…

Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them.

Devices, websites, and networks can collect information about a user’s location.</td><td>Students will be skilled at…

Describing the risks to privacy from collecting and storing personal data on a computer system.

Describing the different types of data that are used and collected by modern computing innovations</td></tr>
</table>

the development and use of software. *NI - Networks & the Internet* 3A-NI-05 - Give examples to illustrate how sensitive data can be affected by malware and other attacks. 3A-NI-06 - Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts. 3A-NI-07 - Compare various security measures, considering tradeoffs between the usability and security of a computer system. 3B-NI-04 - Compare ways software developers protect devices and information from unauthorized access.	*Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.* *Common security risks include: phishing, keylogging, malware, rogue access points* *Methods of protectiong data, including: encryption (symmetrical and asymmetrical), decryption, Caesar Cipher, Random Substitution Cipher, multi-factor authentication.*	Explaining how disparate pieces of personal information can be combined to identify individuals or deduce other private information. Describing the warning signals for common security risks and how they target people – phishing, keylogging, malware, rogue access points, and human error Explaining how computing tools can be used for decryption. Explaining the difference between asymmetrical and symmetrical encryption. Identifing why Caesar Cipher and Random Substitution Ciphers are not adequate for most encryption needs