

# NOVA Cybersecurity Lab Lesson Plan

In this media-rich lesson plan, students explore how to keep their digital lives safe, spot cyber scams, and learn the basics of coding from NOVA Labs. The lesson begins with students watching the Cybersecurity 101 video and discussing the online safety measures that they currently take. Next, students make predictions about online safety best practices, complete the Level 1 challenges of the NOVA Cybersecurity Lab, and compare the best practices from the game with their predictions. Students reconvene for direct instruction on the best practices and key computer science terms, and then finish the Cybersecurity Lab game. Finally, students complete the video quizzes with short-response discussion questions and can work on the Cybersecurity stories as homework reading assignments.

## Lesson Summary

Students explore how to keep their digital lives safe, spot cyber scams, and learn the basics of coding in this media-rich lesson plan from NOVA Labs. The lesson begins with students watching the Cybersecurity 101 video and discussing the online safety measures that they currently take. Next, students makes predictions about online safety best practices, complete the Level 1 challenges of the NOVA Cybersecurity Lab, and compare the best practices from the game with their predictions. Students reconvene for direct instruction on the best practices and key computer science terms and then finish the Cybersecurity Lab game. Finally, students complete the video quizzes with short-response discussion questions and can work on the Cybersecurity stories as homework reading assignments.

## Time Allotment

75 minutes

## Learning Objectives

### Content Objectives

- Students will be able to explain computer science terminology related to coding, password protection, social engineering, and network security
- Students will be able to describe how encryption works to protect privacy
- Students will be able to describe recent network security breaches and how companies defend against them
- Students will be able to explain why the term “hacker” is extremely flexible and describe the variety of roles that hackers play

### Process Objectives

- Students will be able to navigate a robot through a maze game using Blockly code in the Coding Challenge (NOTE: Blockly is a visual interface that uses

puzzle pieces rather than scripted programming language to teach coding. No prior coding knowledge is required.)

- Students will be able to distinguish between phishing attempts, fraudulent websites, and phone scammers in the Social Engineering Challenge
- Students will be able to create strong passwords in the Password-Cracking Challenge
- Students will be able to analyze reports of unfolding security breaches and apply their understanding of security networks to them

## Supplies

- The NOVA Cybersecurity Lab is accessible on web and mobile browsers that support HTML5.

## Multimedia Resources

The lesson plan includes four short videos and an interactive game:

### Cybersecurity 101

<http://mass.pbslearningmedia.org/resource/nvcy-sci-cyber101/cybersecurity-101>

The Internet is fundamentally insecure. However, there are simple things you can do to protect yourself and your information. Learn what they are in NOVA's Cybersecurity Lab.

### Cyber Codes

<http://mass.pbslearningmedia.org/resource/nvcy-sci-cybercodes/cyber-codes>

Do you trust the security of your email, text messages, and browser history? Learn how trustworthy online communication actually is and how encryption can protect your privacy. Sometimes.

### The Secret Lives of Hackers

<http://mass.pbslearningmedia.org/resource/nvcy-sci-slhackers/the-secret-lives-of-hackers>

Hackers may not be who we think they are. In fact, you might be a hacker and not even know it. Learn the true meaning of hacking and some of the many reasons hackers hack.

### A Cyber Privacy Parable

<http://mass.pbslearningmedia.org/resource/nvcy-sci-parable/a-cyber-privacy-parable>

Follow the trials and tribulations of Tim as a seemingly innocent piece of information threatens to ruin his life when it falls into the wrong hands.

### Cybersecurity Lab

<http://mass.pbslearningmedia.org/resource/nvcy-sci-cyberlab/nova-cybersecurity-lab>

This game is designed to help you keep your digital lives safe, spot cyber scams, learn the basics of coding, and defend against cyber attacks.

## Learning Activities

Engage (10 min) – Introduction activity that poses a question or calls upon prior knowledge

- Have students watch Cybersecurity 101 and discuss what they know about cybersecurity and what safety measures they currently take with their online information.

Explore (20 min) – Students explore a hypothesis and collect data

- Challenge students with the question, “How aware are you of the best practices for staying safe online?” Explain to students that in the game, they will explore ways that they can stay safe online and avoid security breaches.
- Instruct students to create a list of tips that they would follow to avoid online scams and to create reliable passwords.
- Instruct students to complete all the Level 1 challenges in the game.

Explain (15 min) – Direct instruction and content delivery

- Reconvene and discuss some of the best practices that students learned. Ask whether they encountered any information that supported or contradicted the tips they compiled before the game.
- Present the best practices and the glossary terms that are essential to understand cybersecurity. Instruct students to take notes.

Elaborate (45 min) – Apply content knowledge and skills to problem (guided practice)

- Instruct students to complete the remainder of the game and to take notes on other best practices they encounter while playing the game.

Evaluate (20 min) – Formal assessment (independent practice)

- Students should complete the video quizzes and turn in their Lab report as their exit slip. <http://www.pbs.org/wgbh/nova/labs/lab/cyber/1/1/>
- Educators should use this opportunity to assess student learning with short-response discussion questions summarizing best practices, the cybersecurity stories, and the glossary terms.

## **Technology Education - PASS Standards**

1.1: Examine the evolution, application and significance of modern technology and its impact on our lives in the twenty-first century.

2: The student will identify the core concepts of technology systems, resources and processes including optimization and trade-off concepts.

4.1: Determine the impact and consequences of technology.

8.1: Identify criteria required to determine an effective technology design process.

9: The student will describe technological advances that enhance science and mathematics and describe how science and mathematics advance technology.

14: The student will identify and describe advances and innovation in the energy-power, biotechnology, **communications**, transportation, manufacturing, construction, and agriculture techniques used to improve each field.

15: The student will identify and describe energy-power, biotechnology, **communications**, transportation, manufacturing, construction, and agriculture technology principles necessary to create products and processes.

18: The student will develop leadership, positive self-concepts, and individual potential in a technological society.

19: The student will explore the organization and management systems of business and industry.

20.1: Examine opportunities related to specific occupations (e.g. career search software, field trips, guest speakers and hands-on activities dealing with lasers, medical, technology, fiber-optics, robotics, biotechnology, computer-aided drafting, electronics, engineering, **computer literacy**, microwave systems, and other technology systems.)

## **Science - Oklahoma Academic Standards (OAS)**

8th grade

MS-PS4-3 Waves and Their Applications in Technologies for Information Transfer

Physical Science

HS-PS4-2 Waves and Their Applications in Technologies for Information Transfer

Physics

HS-PS4-2 Waves and Their Applications in Technologies for Information Transfer

HS-PS4-5 Waves and Their Applications in Technologies for Information Transfer