Digital Defenders: Cybersecurity for K-12 Students

Educator Guide

This course empowers young learners to become safe, smart, and confident digital citizens by teaching them how to protect themselves and their devices in the digital realm. Through interactive lessons and engaging activities, students will gain essential knowledge and skills in cybersecurity.

Learning Objectives

This course is designed for K-12 students with varying levels of cybersecurity knowledge. Students will have the opportunity at the end of this course to explore a variety of worlds in Minecraft Education based on their level of understanding of cybersecurity.

In this course, students will:

- Learn strategies for identifying and responding to common cyber threats;
- Understand basic cybersecurity measures to protect their data and devices;
- Learn how to get help with cybersecurity problems; and
- Apply their knowledge of cybersecurity in one or more Minecraft Education worlds.

Course Format

This self-paced course consists of four lessons. It is designed to take approximately 30-45 minutes to complete, with an additional 1.5 to 5 hours allotted to apply what is learned in Minecraft Education worlds that are tailored to student needs.

Course Overview

Each lesson has embedded reflection questions to help students think more deeply about what they learned and how it applies to them. You can also print or download student-facing materials to support student learning and reflection.

Lesson 1: Understanding the Importance of Cybersecurity

In this lesson, K-12 students are introduced to cybersecurity and its importance to them. Through engaging visuals and relatable stories, they'll gain insight into the current cybersecurity landscape. They'll step into the shoes of cybersecurity experts through role-playing, assessing their own knowledge, and setting personal goals for the course ahead.

Lesson 2: Protecting Yourself

In this lesson, students dig deeper into the world of cybersecurity, focusing on safeguarding their own personal information. They'll learn about the importance of strong passwords and multi-factor authentication (MFA), along with practical steps to create and reset passwords. Students will also become savvy at recognizing phishing attempts and understanding the dos and don'ts of online safety.

Lesson 3: Protecting Your Devices

In this lesson, students learn how to shield their devices and technology systems from digital threats. They'll identify and combat common security risks like malware and ransomware, ensuring their devices are always up to date and backed up. Plus, they'll learn what to do if cyber trouble strikes.

Lesson 4: Explore to Know More

In this lesson, students take the knowledge they've gained throughout the course and apply it through play in virtual Minecraft Education worlds. They'll test their knowledge of cybersecurity awareness and safety to determine which world(s) best meets their individual cybersecurity needs.

Use the Minecraft Education Pathways information to help you determine which pathway is best for individual, small group, or classroom needs. More information, such as learning objectives, downloadable educator guides, and more, can be accessed through the embedded links. Students can use the Reflection Questions found in Lesson 4: Explore to Know More to reflect as they journey through each world.

Vocabulary

- **Authentication** – a method that uses a secret code or key to prove that you are who you say you are when you log in to your accounts.
- **Backup** – making a safe copy of all your important stuff, like your photos or schoolwork, to keep it safe in case something bad happens to your device.
- **Cloud** – an internet storage location where you can keep your files, so you can access them from anywhere with an internet connection.
- **Cybersecurity** – how to keep your devices and personal information safe from bad people who try to do harm or steal your stuff while you're using the internet.
- **Data** – information, such as your pictures, videos, and schoolwork, which you keep on your devices.
- **Devices** – tools you use to access the Internet, like computers, tablets, or smartphones.
- **Malware** – a sneaky computer bug that sneaks into your devices and causes trouble.
- **Personally Identifiable Information (PII)** – your personal details, such as your name, address, or phone number, which can be used to identify you.
- **Phishing** – when someone tries to trick you by sending fake messages that look real, to get your secrets or personal information.
- **Ransomware** – a kind of computer virus that locks up your devices or files and asks for money before you can use them again.
- **Suspicious** – having or showing caution or distrust of someone or something.
- **Update** – a special fix or improvement for your devices or apps to make them work better and keep them safe from problems.

Minecraft Education Pathways

Beginning Cybersecurity

This pathway focuses on how to be a good digital citizen to keep personal data private and be responsible online.

- CyberSafe: Home Sweet Hmm
  Time needed: 1.5 hours
- Privacy Prodigy
  Time needed: 1.5 hours

Mid-Level Cybersecurity

This pathway challenges students to protect a school network against attackers and prepares them with help from cybersecurity experts to prevent large attacks.

- Cyber Fundamentals (Part 1): Network Heroes
  Time needed: 2 hours
- Cyber Fundamentals (Part 2): The Interceptors
  Time needed: 1.5 hours
- Cyber Fundamentals (Part 3): Cloud Champions
  Time needed: 1.5 hours

Advanced Cybersecurity

This pathway empowers students to explore how to stay safe in today's digital world to prepare for future careers and support real-world problem-solving. They'll attempt to ward off complex attacks, investigate damage to systems, and implement techniques to remove malicious code.

- Cyber Expert (Part 1): Cryptic Ciphers
  Time needed: 1.5 hours
- Cyber Expert (Part 2): Daring Defense
  Time needed: 1.5 hours
- Cyber Expert (Part 3): Malware Mayhem
  Time needed: 1.5 hours
- Cyber Defender
  Time needed: 0.5 hours

Digital Defenders: Cybersecurity for K-12 Students

Student Materials

Download or print these materials to support student learning and reflection.

Reflection Questions

Lesson 1: Understanding the Importance of Cybersecurity

Answer these questions as you reflect on what you learned in Lesson 1.

- In your own words, what is cybersecurity?

- Write or draw an example that shows your understanding of cybersecurity.

Describe why learning about cybersecurity is important to you in each of these areas:

- Digital citizenship

- Data privacy

- Future careers

- What questions do you have for your teacher or school staff about cybersecurity?

Lesson 2: Protecting Yourself

Answer these questions as you reflect on what you learned in Lesson 2.

- In your own words, what is phishing? How do cybercriminals try to trick you into revealing your personal information?
- Why is it important to slow down, review, and think before responding to a suspicious message? What can happen if you don't? What are some of the red flags you should look for in an email or text message?
- Why should you use strong and unique passwords for each of your online accounts? What makes a password strong?
- If you receive a message that you think is a phishing attempt, what steps should you take to protect yourself and your information?

What questions do you have for your teacher or school staff about phishing? What questions do you have about multi-factor authentication, passwords, or reporting procedures at your school?

Lesson 3: Protecting Your Devices

Answer these questions as you reflect on what you learned in Lesson 3.

- In your own words, what is malware? Why is it important to be cautious about it when using your devices?

- List or draw examples of the problems malware can cause and common signs that your device might be infected.

- In your own words, what is ransomware? Why is it important to avoid opening strange emails or clicking on suspicious links?

- If you suspect there is a problem with your computer, like malware or ransomware, what should you do to address the issue? Who should you contact for help?

  What questions do you have for your teacher or school staff about malware or ransomware? What questions do you have about device updates and backups at your school?

Lesson 4: Explore to Know More (Beginning Cybersecurity)

Use these questions to reflect on your experience during and after playing the Minecraft Education worlds.

CyberSafe: Home Sweet Hmm

- Name one positive thing about the internet.
- Name one risk that can happen on the internet.
- How can you stay safer on the internet?
- Why is it important to protect your personal information?

Privacy Prodigy

- What are the different types of personal data? With whom should you share your personal data?
- How can you protect your personal data?
- Why is it important to protect your privacy and personal data?

Lesson 4: Explore to Know More (Mid-Level Cybersecurity)

Use the questions to reflect on your experience during and after playing the Minecraft Education worlds.

Cyber Fundamentals (Part 1): Network Heroes

- What components make up a local-area network (LAN)?
- How are a local area-network (LAN) and wide-area network (WAN) different from one another?
- How can you create a complex password?
- Why are complex passwords important in cybersecurity?
- Name one other way to keep a network safe.
- What is malware?
- How can you protect yourself from malware?
- How do phishing scams work?

Cyber Fundamentals (Part 2): The Interceptors

- What are some examples of multi-factor authentication?
- Where in your life could multi-factor authentication make things safer?
- What is an incident response team?
- What are some of the roles of an incident response team and what do they do?
- In your own words, describe what happens during a cybersecurity incident.

Cyber Fundamentals (Part 3): Cloud Champions

- What are some of the risks of oversharing personal information on social media?
- In your own words, what do the numbers in the 3-2-1 back-up method represent?
- Describe how you could use the 3-2-1 back-up method at home or school.
- What are some examples of Internet of Things (IoT)?
- What are the risks and benefits of IoT?
- Why is cybersecurity important?
- What are the cybersecurity practices you could use in your life?

Lesson 4: Explore to Know More (Advanced Cybersecurity)

Use the questions to reflect on your experience during and after playing the Minecraft Education worlds.

Cyber Expert (Part 1): Cryptic Ciphers

Define the terms:

- Encryption
- Decryption
- Message Integrity
- Social Engineering

Cyber Expert (Part 2): Daring Defense

Define the terms:

- Firewall
- DDos Attack
- Access Control

Cyber Expert (Part 3): Malware Mayhem

Define the terms:

- Honeypot
- Antivirus
- Ransomware

Cyber Defender

- Provide some examples of common cybersecurity threats.
- What should you consider when selecting and implementing cybersecurity measures?
- How do we achieve balance for organizations as it relates to cybersecurity?
- What skills are needed in cybersecurity fields and careers?