sphero

BOLT™

CYBERSECURITY LABS

EDUCATOR GUIDE

CONTENTS

INTRODUCTION

Our increasingly digital society puts the world at our fingertips, allowing us to learn practically anything, communicate and collaborate with people on the other side of the globe, and innovate solutions to our biggest challenges. Unfortunately, the digital world opens us up to an entirely new and scary set of threats. The demand has never been greater for a robust cybersecurity workforce and citizens with a strong understanding of computer ethics and how to protect their digital lives.

The Sphero BOLT Cybersecurity Labs aim to address this challenge by bringing cybersecurity concepts to life through hands-on learning experiences. BOLT simulates and models concepts that are often hidden deep inside computers, networks, and code so that middle school students can visualize, discuss, and fully understand them.

The labs were developed in collaboration with **Dr. Pauline Mosley**, Full Professor and Associate Chair of Information Technology at Pace University. Dr. Mosley's subject matter expertise ensures the learning in the labs is both accurate and current. At the same time, as the director of **Camp Cryptobot**, her enthusiasm for engaging more middle and high school students in cybersecurity career pathways ensures the labs are relevant, high-interest, and, most importantly, fun!

Objectives

By the end of the unit, students will be able to:

- explain how computers use private and public networks to transmit information
- differentiate between ethical and unethical uses of technology
- evaluate the risks and benefits of different computing practices
- identify different types of hackers and explain their motives
- identify and explain common cyber attacks including phishing, malware, distributed denial of service attacks, and more
- explain techniques that cybersecurity professional use to protect internet connected devices and computer users
- share strategies for keeping themselves and their devices safe from common cyber attacks
- describe potential career paths in the field of cybersecurity

THE SPHERO MISSION

Sphero is transforming PK-12 education with accessible tools that encourage exploration, imagination, and perseverance through STEAM and computer science. With the help of educators around the world, we are empowering learners of all backgrounds and abilities to discover their interests and passions while equipping them with the skills they need to be the world's future Changemakers.

DEAR EDUCATORS,

WELCOME TO CYBERSECURITY LABS!

Cybersecurity is quickly becoming a priority as young minds are learning STEM and prepare to join the workforce in this age of information and rapid globalization. According to data collected by the U.S. Bureau of Labor Statics (BLS), the demand for cybersecurity jobs like information security analysts will grow by as much as 33% over the next ten years. Yet, data from the National Center for Women and Information Technology (NCWIT, 2010), only about 3% of the available pool of minority high school graduates will earn computing degrees from American colleges and universities, thus lacking the qualifications to fill these jobs. Recognizing the urgent need to expand the workforce pool of cybersecurity professionals in the next 20 years—in particular with people from underrepresented groups—the Sphero BOLT Cybersecurity Labs begin both an education and cybersecurity pipeline restoration initiative.

The Sphero BOLT Cybersecurity Labs is a standards-aligned set of guided hands-on experiences that introduce students to cybersecurity principles, ethics, and techniques. The labs, utilizing multiple entry points and connections to relevant topics in students' everyday lives, will help to create a strong cybersecurity foundation for students that can be used to improve their digital hygiene and start them on a pathway to a cybersecurity career. A major strength of this curriculum is the differentiation of activities for diverse skills sets, young women and minorities. Labs can be easily modified for these students with diverse skill sets so that the delivery of the content is inclusive and engaging while cultivating self-efficacy—a critical factor in student success.

It is our desire that students who interact with these labs will feel empowered with knowledge, technological skill sets, and a mindset that there is nothing that you cannot do if you put your mind to it. Enjoy yourself, ask questions, make mistakes, make friends, and most importantly—we demand that you have fun!!

Sincerely,
Dr. Pauline Mosley
Pace University
Full Professor and Associate Chair of Information Technology
Director of Camp CryptoBot

LAB FEATURES

Designed for Middle School Students

The labs are designed specifically to introduce middle school students to the field of cybersecurity with two primary goals. First, the labs teach and reinforce the principles of digital hygiene and ethical computing use so students know how to keep themselves and their community safe. Second, the labs showcase how illegal hackers commonly attack networks and devices as well as the steps that cybersecurity professionals take to stop attacks so that students build a foundation for going deeper into cybersecurity education and careers.

Focused on Cybersecurity

The focus of the labs is on cybersecurity, not on teaching computer programming skills. Provided pre-created programs allow students to interact with the cybersecurity concepts out-of-the-box without any previous programming experience. However, students will get more out of the labs if they have some previous experience with block coding and with BOLT robots. We strongly recommend completing the Intro to Blocks activities in the Sphero Edu app before completing the cybersecurity labs.

Easy to Differentiate and Extend

Use the ideas and resources in the educator notes to help adapt the labs to the experiences and needs of your students. You'll find links to instructional ideas, resources, and videos as well as ideas for taking students' learning further.

Tied to Career Pathways

The labs highlight how cybersecurity professionals work to keep us and our computing devices safe from cyber threats and broaden students' horizons to consider future cybersecurity careers. In the final lab, students explore different career options and research and present their findings to their peers.

Aligned to Cybersecurity Standards

The labs are aligned to the K-12 Cybersecurity Learning Standards—developed in 2021 by Cyber.org and educators across the United States—to "increase student cybersecurity literacy and build a robust pipeline of future cybersecurity talent." The standards are organized into three core themes: Computing Systems (CS), Digital Citizenship (DC), and Security (SEC).

Theme: Computing Systems (CS)

- **6-8.CS.APPS** Discuss the role that software plays in the protection of a secure system.
- **6-8.CS.CC** Identify the advantages and disadvantages of various cloud computing models.
- **6-8.CS.COMM.1** Compare and contrast network topologies.
- **6-8.CS.COMM.2** Differentiate between a network device's MAC and IP addresses.
- **6-8.CS.COMP** Identify the role of connected network components.
- **6-8.CS.HARD** Develop strategies to raise awareness of hardware vulnerabilities.
- **6-8.CS.IOT** Evaluate the risks and benefits of the Internet of Things devices.
- **6-8.CS.LOSS** Explain the role and importance of backups.
- **6-8.CS.OS** Discuss the risks of outdated operating systems.
- **6-8.CS.PROG** Explain the role of scripting in cyber attacks.
- **6-8.CS.PROT** Identify the protocol connection types used for different services available online.
- **6-8.CS.SOFT** Identify examples of vulnerabilities that exist in software.

Theme: Digital Citizenship (DC)

- **6-8.DC.AUP** Understand the various agreements and how they protect users and owners of technology.
- **6-8.DC.CYBL** Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying.
- **6-8.DC.ETH** Distinguish between ethical and malicious hacking.
- **6-8.DC.FOOT1** Recognize the many sources of data that make up a digital footprint.
- **6-8.DC.FOOT2** Recognize the permanence of a digital footprint.
- **6-8.DC.IP** Explain how intellectual property and copyright relate to fair use.
- **6-8.DC.LAW** Analyze specific federal, state, and local laws as they relate to cybersecurity and privacy.
- **6-8.DC.PP.1** Discuss the risks and benefits of sharing PII.
- **6-8.DC.PP.2** Examine techniques to detect, correct, and prevent disclosure of PII.
- **6-8.DC.THRT** Describe various types of threat actors.

Theme: Security (SEC)

- **6-8.SEC.ACC** Explain the concept of access control and how to limit access to authorized users.
- **6-8.SEC.AUTH** Explain how authentication and authorization methods can protect authorized users.
- **6-8.SEC.CIA** Explain the effects of a failure of the CIA Triad.
- **6-8.SEC.COMP** Describe Defense in Depth strategies to protect simple networks.
- **6-8.SEC.CRY** Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.
- **6-8.SEC.CTRL** Describe Defense in Depth and how physical access controls work together.
- **6-8.SEC.DATA** Describe data in its three states and potential threats to each state.
- **6-8.SEC.INFO** Analyze threats and vulnerabilities to information security for individuals and organizations.
- **6-8.SEC.NET** Explain how malicious actions threaten network security.
- **6-8.SEC.PHYS** Explain how malicious actions threaten physical security.

LAB STRUCTURE

Each lab uses the following structure to engage students and develop a deeper understanding of cybersecurity concepts:

Activate

In **Activate Steps**, labs make connections to prior knowledge that students may already possess about the topic and engage student interest.

Learn

In **Learn Steps**, the labs provide core learning vocabulary and concepts to enable students to grow their cybersecurity understandings. Use the ideas and information in the educator notes to take this learning further.

Investigate

In **Investigate Steps**, students open and execute a BOLT program to start to explore the topics in a hands-on manner.

Hack

In **Hack Steps**, students modify the program to extend the model through additional scenarios and gameplay.

Secure Your Understanding

In **Secure Your Understanding Steps**, students connect the BOLT model back to computing in their everyday lives and discuss their cybersecurity learnings with their classmates.

FACILITATION TIPS

Before Teaching:

- Read through the student instructions for the activity, try out the programming, and anticipate obstacles that your students may encounter.
- Read the educator notes in the Lab Steps and consider points where you will pause students for whole-class instruction and discussion.
- Prepare your classroom space for the needs of the lab according to student instructions and educator notes.
- Determine whether the lab uses IR communications between two or more groups and, if needed, plan for larger student groups with two or more BOLTS and programming devices.
- Make sure all robots and programming devices are fully charged.
- Plan for two students per BOLT robot.

During Teaching:

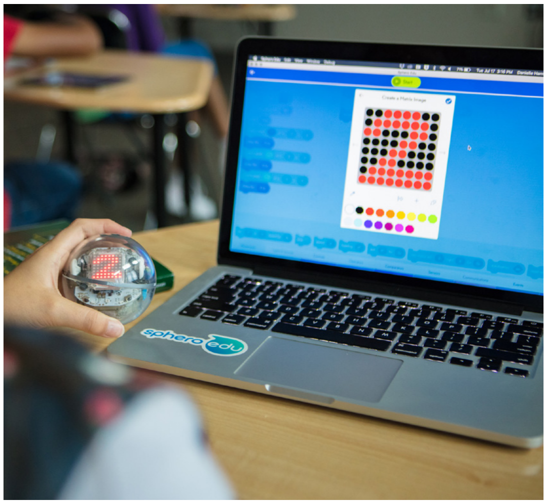
- Circulate your classroom space to troubleshoot challenges with students. If multiple groups are struggling with the same problem, troubleshoot it as a whole class.
- Use the educator notes for potential student solutions as well as ideas on how to extend challenges and learning.
- Consider time. If possible, reserve 5–10 minutes at the end of your instructional period for the Secure Your Understanding Step.

After Teaching:

- Reflect on student learning. What was easy for students? What was difficult? Was there an artifact of student learning that you can share with the whole class to address a common challenge or showcase a programming concept or problem solving strategy?
- Explore how you can use ideas and resources in the lab and/or educator notes to deepen student learning.
- Consider how you could build the topic into an independent or group project. For example, students could research another example of a phishing scheme and present their learning to their peers.

LAB GROUPINGS

The cybersecurity labs are broken down into **four levels**—red, yellow, blue, and green—each with **five labs**. The labs are presented in a loose **sequential order**, starting with the most introductory cybersecurity concepts and ending with some of the most advanced. You can start at Red 1 and teach all the way to Green 5. However, each lab is also meant to **stand alone**. You can **pick and choose** topics that are most relevant to your students' needs and your curriculum. Pay close attention to the **coding prerequisites**, if any, listed in the description of the lab when planning.



RED LEVEL
ETHICS AND NETWORKS

Students start their cybersecurity journey by learning about ethical vs. unethical computing practices and consider a computing code of ethics. Then students learn the basics of how computers communicate via the internet and on private networks. The digital footprint labs trace students' paths through the internet and introduce ways that their digital actions are tracked (and used) by others.

Click each title or activity name to view the activity in the Sphero Edu app

RED 1 *The Ethics of Computing: Right vs. Wrong*

A strong code of ethics forms the heart of cybersecurity, influencing the choices we make when using our computing devices as well as how we protect ourselves and others from cyber threats.

By the end of this lab, students will be able to:

- explain a Code of Ethics for computer professionals.
- differentiate between an ethical and unethical decision.

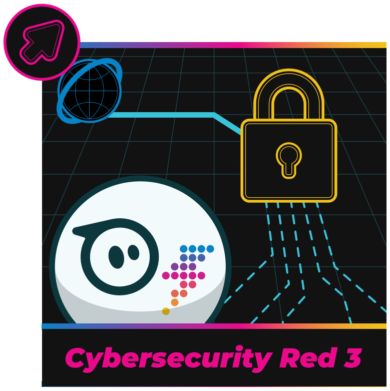
RED 2 *How the Internet Works: The Big Picture*

Most of us use the internet daily for work, school, and life. But what exactly is the internet and how does it work?

By the end of this lab, students will be able to:

- describe IP and TCP protocols.
- use BOLT robots to explain how the internet works.
- compare and contrast websites that use HTTP and HTTPs.

RED 3 *Private Networks: Keeping it Private*



The internet is a vast, public space, but odds are, you spend most of your time accessing the internet from a private network called a local area network (LAN) whether you are at home, at the library, or in school.

By the end of this lab, students will be able to:

- define and diagram a Local Area Network (LAN).
- describe the role of a modem and router.
- explain how firewalls protect devices on a LAN from the public internet.

RED 4 *Digital Footprints: Our Internet Tracks*

Just like a footprint in the ground, digital footprints can be used to track your decisions and movements online. It's important for you to start thinking about this as soon as you start using the internet.

By the end of this lab, students will be able to:

- Identify what a digital footprint is.
- Create a model of a digital footprint as a class.
- Look into what is currently in their digital footprint.

RED 5 *Managing Your Digital Footprint*

Understanding how your digital footprint is created and what it is used for is critical to protecting yourself and your information. While many parts of your digital footprint can be harmless—and even useful—without proper attention it can quickly turn into a lot of information that you do not want anyone to have access to.

By the end of this lab, students will be able to:

- Identify what types of information could be included in a digital footprint.
- Decide what pieces of information they would want and not want in their digital footprint.
- learn techniques on how to control their digital footprint.

YELLOW LEVEL
CYBERBULLIES AND HACKERS

Students revisit the concept of ethical computing with a focus on cyberbullying. They then learn about the different types of hackers; in addition to unethical/illegal hackers, there are also ethical/legal hackers that spend their days countering the bad actors. Students explore some ways that bad actors use phishing and social engineering to plant viruses and worms - two types of malware that can cause harm.

Click each title or activity name to view the activity in the Sphero Edu app

YELLOW 1 *Cyberbullying: Don’t Be a Bully*

Cyberbullying can have incredibly negative effects on not only the victim but also the person that engages in cyberbullying and entire online communities.

By the end of this lab, students will be able to:

- explain the definition of cyberbullying.
- discuss the effects cyberbullying has on mental health.
- explore different ways you can prevent cyberbullying.

YELLOW 2 *Types of Hackers: To Hack or Not to Hack*

The good, the bad, and everything in between. The cybersecurity world is filled with all types of hackers with a wide variety of motivations.

By the end of this lab, students will be able to:

- explain the definition of hacking.
- discuss the legal and ethical consequences of hacking.

YELLOW 3 *Phishing: How Illegal Hackers Find You*

Phishing and social engineering are common techniques that unethical hackers use to convince unsuspecting people to give their information freely, and then use it to gain access to their passwords, bank accounts, credit card information, and more.

By the end of this lab, students will be able to:

- explain the definition of phishing.
- discuss the dangers of phishing, hoaxes, and social engineering.
- discuss different ways you can protect yourself from falling victim to phishing.

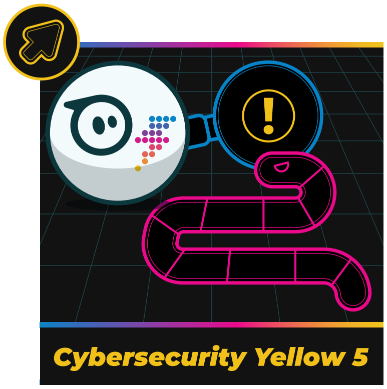
YELLOW 4 *Virus: Modeling the Spread of a Computer Infection*

Malware, or malicious software designed to damage and disrupt our technology, is, unfortunately, a fact of modern life. However, learning what it is and how it works can help us all keep our computers and ourselves safer.

By the end of this lab, students will be able to:

- describe the three main types of malware.
- model how malware like a virus spreads with BOLT.
- describe steps individuals and cybersecurity professionals take to combat malware.

YELLOW 5 *The Morris Worm: Historical Malware*



Just like a physical worm, computer worms can wriggle, spread, and grow across a network, infecting computers as they go. While sometimes harmless, many worms are malicious malware that can damage computers and create possibilities for attacks.

By the end of this lab, students will be able to:

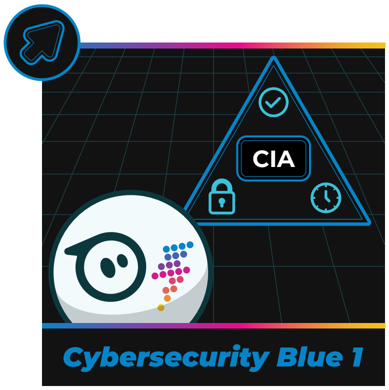
- compare and contrast worms and virus.
- model the Morris Worm with a BOLT program.
- describe the types of harm worms can cause.

BLUE LEVEL
CIA TRIAD AND ATTACKS

Students learn about the CIA Triad model, used by cybersecurity professionals to plan for information security. They then learn about other bad actor threats including DDoS attacks, sniffing and scanning, and person-in-the-middle attacks. Woven into each are strategies used by legal hackers to counter the threat and ensure information availability, integrity, and confidentiality.

Click each title or activity name to view the activity in the Sphero Edu app

BLUE 1 *CIA Triad: Planning for Security*

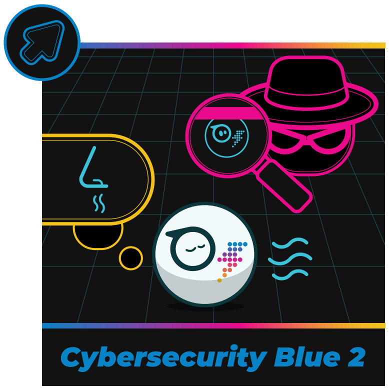


When planning for information and network security, cybersecurity professionals keep the CIA Triad—Confidentiality, Integrity, and Availability—at the core of their decision making.

By the end of this lab, students will be able to:

- explain the meaning of Confidentiality, Integrity, and Availability in the CIA Triad.
- describe the role of each principle in the CIA Triad in protecting information and data.

BLUE 2 *Hacker Snooping: Sniffing and Scanning*



Before a hacker can attack you, they have to learn about your vulnerabilities. Cybersecurity criminals use two reconnaissance techniques to learn about your vulnerabilities: sniffing and scanning.

By the end of this lab, students will be able to:

- describe the difference between sniffing and scanning.
- explain how attackers weaponize information they gather about computing systems.
- use IR messages to take over an opposing team's BOLT.

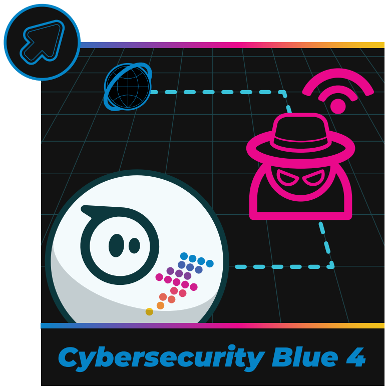
BLUE 3 *Denied: Denial of Service Attacks*

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are some of the more common and disruptive cyber attacks. Relatively inexperienced cybercriminals can take down large websites, making information and services unavailable.

By the end of this lab, students will be able to:

- describe Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- program two BOLTs to represent the attacker and the victim in a DoS attack.
- modify the program to reduce your BOLT's susceptibility to a DDoS attack.

BLUE 4 *Person-in-the-Middle Attacks: Who's There?*



A person-in-the-middle attack sounds exactly like what it is: an illegal hacker intercepting communications between you and the internet services you use while on a computer.

By the end of this lab, students will be able to:

- describe a person-in-the-middle attack.
- model a person-in-the-middle attack with BOLT robots.
- explain how to keep themselves safe while using internet-connected computers.

BLUE 5 *Circles of Influence: Authenticate & Authorize*

To distinguish between different types of users, different types of user authorization can be used. When this authorization is compromised, it can have chaotic consequences.

By the end of this lab, students will be able to:

- define authentication and its importance in cybersecurity.
- discuss the four general means of authenticating a user's identity (password, biometric, electronic, smart cards).
- model authorization levels with BOLT.
- describe some of the key security issues for user authentication.

GREEN LEVEL
CRYPTOGRAPHY AND YOUR FUTURE

In the final level, students dig deeper into the world of cybersecurity professionals and examine how passwords and information encryption can keep our digital information and lives safe. In the final lab, after developing an initial understanding of many cybersecurity topics, students preview job opportunities in the world of cybersecurity.

Click each title or activity name to view the activity in the Sphero Edu app

GREEN 1 *p@$$W0RD$!: What's Behind a Strong Password*

Which is more mighty: a human or a machine? Well, when it comes to cracking passwords, computers are much faster than we are.

By the end of this lab, students will be able to:

- use BOLT to crack a combination lock.
- describe two methods illegal hackers use to crack passwords.
- explain how to form strong and memorable passwords.

GREEN 2 *Intro to Cryptography: Pigpen Cipher*

Have you ever passed notes in a secret code? Well, computers communicate all the time in encrypted messages.

By the end of this lab, students will be able to:

- use BOLT and the pigpen cipher to send secret messages to your classmates.
- explain how plaintext is encrypted into ciphertext and then decrypted back into plaintext.
- encrypt and decrypt messages with BOLT and the pigpen cipher.

GREEN 3 *The Caesar Shift: Caesar Says What?!*

In the words of the ancient Roman leader, Julius Caesar, “RljvnRbjfRlxwzdnanm.” Wait, what?!?! Turns out Caesar often encrypted his communications and one of the most well-known of all ciphers, the Caesar Shift, is named after him.

By the end of this lab, students will be able to:

- encrypt and decrypt messages with the Caesar Shift.
- manipulate a JavaScript BOLT program to explore cryptography.
- identify the characteristics of strong ciphers.

GREEN 4 *Multiply It! Modulo Arithmetic & Ciphers*

Learn about the multiplication cipher, a monoalphabetic cipher. In the process, you’ll become comfortable with modular arithmetic and begin to understand its importance to modern cryptography.

By the end of this lab, students will be able to:

- encrypt and decrypt messages with a multiplication cipher.
- use the modulo operation to calculate the remainder.

GREEN 5 *Cybersecurity Career Parade*

Incident responders, cryptographers, penetration testers; One of these could be your job title in the future.

By the end of this lab, students will be able to:

- identify different cybersecurity careers.
- understand where and what careers are in high demand.
- explain details of a cybersecurity career of their choosing.

TECHNOLOGY TIPS

The Sphero Edu App

Download the The Sphero Edu app here.

Create Classes and Assign Activities

Create a teacher account so you can set up and manage classes as an educator. You have a few options for managing your classes:

- **Class Codes (Recommended)**

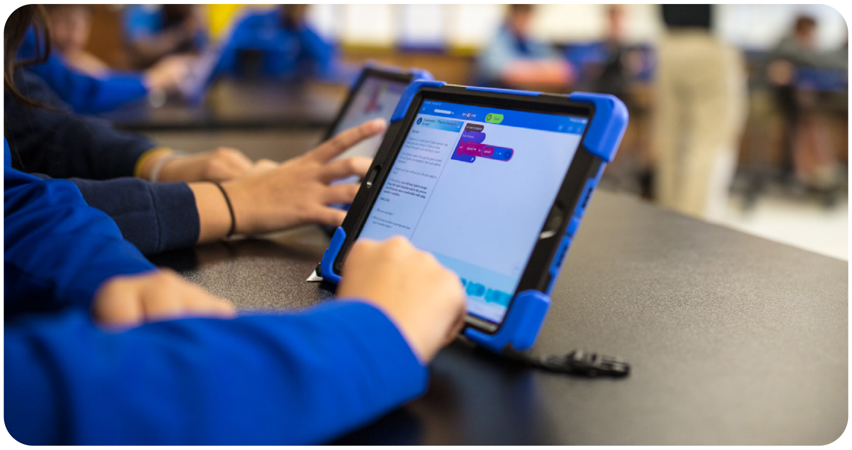
  If you prefer for students to work on assignments without a username and password, distribute Class Codes. Simply enter a Class Name and the class code will generate automatically. Give students the class code to access their assignments and continue working on their programs. Unlike standard classes, student progress is saved to the class rather than an account. Learn more **here**.

- **Standard Class**

  Create students accounts manually or by uploading a CSV. These student accounts include individual usernames and passwords for each student. In this model, you can assign activities to students for completion, but cannot directly assign programs. All student work is saved to their personal account and not the class itself.

- **Google or Clever users**

  You can automatically sync your classes to Sphero Edu. View more information **here**.



Charging Robots

Sphero BOLT robots charge via inductive charging in the provided cradle. To charge, place your robot on the charging cradle heavy side down. You will see a blue light blinking on the cradle to indicate it is charging. BOLT will need up to 6 hours for a full charge, but time will vary depending on the battery's current level and you will know it's charged when the blue light stops blinking.

Troubleshooting

- Make sure the robot firmware is updated. If a firmware update is required, it will begin automatically after it is connected to a device.
- Charge robots and devices the night before using them in class.
- Make sure the Sphero Edu app is up-to-date.
- Restart your Sphero robot by holding the button down on the charger and removing the robot from the charging cradle, then place it back on the charging cradle.

Support

Sphero is empowering the future creators of tomorrow and setting them up for success. We couldn't be more excited about the future of education and the part we're playing. For more information about Sphero and to get involved in our community you can find links to additional resources below.

- **Sphero Blog -** Visit our **education blog** for updates, tips, and suggestions.
- **Support -** Visit our **support page** for FAQ and troubleshooting tips and tricks.
- **Contact Us -** For any additional support or help contact us **here**.