Code.org Personal Security Resources

Grade Level: K-5

Safety in my Online Neighborhood

Computer Science Fundamentals Course A, Lesson 1 (Grade level: K)

The power of the internet allows students to experience and visit places they might not be able to see in person. But, just like traveling in the real world, it's important to be safe when traveling online. On this virtual field trip, kids can practice staying safe during online adventures.

Digital Trails

Computer Science Fundamentals Course B, Lesson 1 (Grade level: 1)

Does what you do online always stay online? Students learn that the information they share online leaves a digital footprint or "trail." Depending on how they manage it, this trail can be big or small, and harmful or helpful. Students compare different trails and think critically about what kinds of information they want to leave behind.

Password Power-Up

Computer Science Fundamentals Course D, Lesson 1 (Grade level: 3)

Stronger, more secure online passwords are a good idea for everyone. But how can we help kids create better passwords and actually remember them? Use the tips in this lesson to help kids make passwords that are both secure and memorable.

Private and Personal Information

Computer Science Fundamentals Course E, Lesson 5 (Grade level: 4)

It's in our students' nature to share and connect with others. But sharing online comes with some risks. How can we help kids build strong, positive, and safe relationships online? Help your students learn the difference between what's personal and what's best left private.

Grade Level: 6-10

Digital Footprint

Computer Science Discoveries Unit 2, Lesson 5

This lesson is part of a unit in which students develop web pages, and is designed to help them articulate what personal information they choose to share digitally and with whom.
Students look at several social media pages to determine what information people are sharing about themselves or one another, and reflect on what guidelines they think are appropriate for posting information online.

Code.org Personal Security Resources

Grade Level: 9-12

The following lessons are from Computer Science Principles Unit 10, which is focused on cybersecurity and global impacts.

Data Policies and Privacy
Computer Science Principles Unit 10, Lesson 3
Students learn that the apps, websites, and other computing innovations they use every day require a lot of data, much of which they might consider to be private or personal. Students read data policies from a website or service they use or know about. This investigation focuses on the kinds of data that are being collected, the way it's being used, and any potential privacy concerns that arise. A brief second activity reveals that even data that may not seem private, like a birthdate or zipcode, can be combined to uniquely identify them.

The Value of Privacy
Computer Science Principles Unit 10, Lesson 4
Students develop their own opinions on the privacy tradeoffs inherent in many modern computing innovations. At the beginning of the lesson students watch a video on facial recognition technology that presents the tradeoffs between convenience and privacy. Students also respond to two additional videos that look at tradeoffs between privacy, security, and convenience. Students then evaluate a website or app they investigated in the previous lesson to determine if they think the benefits of the service outweigh the privacy risks.

Security Risks 1 and 2
Computer Science Principles Unit 10, Lessons 6 and 7
Students investigate three different common security risks (phishing, keylogging, malware) in a jigsaw activity. In groups, students create Public Service Announcement slides warning of the dangers of their assigned security risk. The second lesson begins with a review of security risks by watching a video on cybersecurity and crime. Following this, the class does an investigation into the Equifax breach, and what went wrong. The class ends with a quiz to review security risks.

Protecting Data 1 and 2
Computer Science Principles Unit 10, Lessons 9 and 10
In the first lesson of this series, students explore two different encryption widgets: The Caesar Cipher Widget and the Random Substitution Cipher. Afterwards, students watch a video that reviews these types of encryption and introduces a new concept: public key encryption. The second lesson is a guided tour of multifactor authentication and software updates that students can use to protect their data.