Cybersecurity

About the Lessons

The three lessons in this unit are designed to introduce students to cybersecurity concepts. Each lesson lasts 20 or 30 minutes.

The lessons are designed to be taught in order:

- **Lesson 1: The Value of Information**

Students brainstorm examples of personally identifiable information and consider how people can use this information in good or bad ways.

- **Lesson 2: What Is a Cyberattack?**

Students act out a model of how information travels on the Internet, then use the model to explore how cyberattacks work.

- **Lesson 3: Keeping Our Information and Ourselves Safe**

Students explore methods to protect information from cyberattacks, consider ways to keep themselves and others safe online, and learn about cybersecurity careers. In an optional extension, students explore encryption methods and the ways in which they keep data secure.

The Value of Information

Overview

Students examine precipitation data to draw conclusions about the changes in Earth's climate since the 1960s. A video introduction discusses how increased temperatures have caused more extreme precipitation. Students then explore their local environments to suggest methods for mitigation of greenhouse gas emissions and adaptation to extreme precipitation.

A more advanced version of this lesson is available in *Climate Change,* Gr 6-8.

Guiding Question

What is personally identifiable information and why is it valuable?

Objectives

Students will be able to

- define *data*.
- define and give examples of personally identifiable information.
- explain why personally identifiable information is valuable.

Time

- 20 minutes

Grade Level: 6–8

Vocabulary

- **Attacker**
- **Data**
- **Information**
- **Personally Identifiable Information**
- **Trade-off**

Standards

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

Background

A central concept in the field of cybersecurity is personally identifiable information (PII). Personally identifiable information includes basic, commonly shared information such as a person's name, family members' names, birthdate, physical address, telephone number, email address, social media usernames, and associated institutions such as schools and employers. It also includes private, rarely shared information such as a person's Social Security number, health information, passwords, and financial information such as bank accounts and credit card numbers.

PII has many beneficial purposes. For example, it allows people to connect with friends and family, get healthcare, and make purchases. However, it can also be used for malicious purposes. For example, an attacker can use someone's private PII to steal from or impersonate them. Even basic, commonly shared PII can pose a danger if an attacker uses it to harass someone, stalk them, or guess their passwords

or account information. These dangers make it important to keep personally identifiable information secure and share it only when necessary.

When information is stored on a computer, it is called data. Storing PII as data can be convenient. However, networked computers (such as those connected to the Internet) have weaknesses that make it possible for attackers to access and misuse PII stored as data.

Materials

For the educator:

- A way to create and view a list as a class (e.g., whiteboard, chart paper, shared document)

For each small group:

- 1 common object such as a slip of paper, craft stick, or index card to identify the team (blue for half the groups, red for the other half)

For each student:

- 1 copy of *Personally Identifiable Information* (English | Spanish Coming Soon | Answer Key)
- 1 pencil

EiE® Connections

Learn more about the Engineering Design Process in the EiE Video Library.

Continue your classroom activities with these units:

Computer Science Essentials™

- Building Automated Systems
- Designing Computer Games
- Analyzing Digital Images

Note that the Computer Science Essentials™ series is part of Engineering and Computer Science Essentials™: An Integrated Program.

Museum of Science Connections

Listen to the Pulsar podcast episode "What Is Data?" (10 minutes)

Explore the interactive infographics "Defending the Internet" and "AI Is All Around Us."

Family Connections

Continue the learning at home with this activity:

Careers for Engineers Quiz

Credits

This lesson is offered at no cost thanks to the generosity of the Akamai Foundation.

Activity Instructions

1. Explain to students that they are about to start exploring two important concepts: the Internet and security. Ask the following questions to get them thinking about these concepts and assess their prior knowledge:

> **Q: What is the Internet?**
>
> *A: Accept all responses. Students may describe the computers they use to access the Internet, such as laptops, phones, and video game consoles; the content they access on the Internet, such as media and games; the ways the Internet is connected, such as through wires or Wi-Fi; or the Internet as a "space" or "place."*

> **Q: How can we be safe when using the Internet?**
>
> *A: Accept all responses. Possible responses include not giving out our real names, not communicating with strangers, and visiting only safe websites.*

Record students' responses with words or drawings on a whiteboard, chart paper, or in some other medium for reference throughout the lessons.

2. Tell students that today they will be thinking about how to provide online security for themselves, their families, their classmates, and their communities. Specifically, they'll be thinking about something that is important to secure: information. Ask:

> **Q: What is information?**
>
> *A: Accept all responses. Responses may include facts, details, or knowledge. Students may suggest types of information, such as visual, numerical, or geographic, or examples of information in their own lives, such as family recipes or stories.*

As necessary, explain to students that ***information*** refers to facts of any kind.

3. Tell students that today, they will be thinking about a specific type of information: **personally identifiable information**, or facts that can be used to identify a particular person. As needed, mention a few types of personally identifiable information, such as name and telephone number.

4. Organize students (or have them organize themselves) into small groups. Give each student a copy of *Personally Identifiable Information* (English | Spanish Coming Soon). Explain that groups will work together to think of different kinds of personally identifiable information, then list the kinds of information they think of in the left column of the sheet. Give students about five minutes to brainstorm.

Activity Tips

Students can share ideas in whatever way is best for them. This may include writing or drawing on Personally Identifiable Information, speaking to classmates, or using other media such as audio and video recordings.

Make sure students understand that they are listing types of personally identifiable information, not sharing actual PII.

Material Tips

You can circulate to see and hear students' ideas as they work, then record those ideas on chart paper, a whiteboard, or some other medium for the whole class to reference during further discussion.

5. Have groups share some examples of personally identifiable information that they brainstormed. Choose one familiar example to focus on as a class, such as home address, email address, or telephone number.

6. Using the selected example, ask:

Q: What are some good, nice, or helpful ways to use this information?

A: Responses will vary. A possible response: I can use the home addresses of friends and family members to send them letters and packages and visit them.

7. Using the same example, ask:

> **Q: What are some bad, mean, or criminal ways to use this information?**
>
> *A: Responses will vary. A possible response: I can use someone's home address to send them mean letters or stalk them.*

8. Explain to students that personally identifiable information is valuable because it can be used in both good and bad ways. Tell them that they will divide into teams to explore these uses further. Emphasize, however, that the teams are not in competition. All students have the same goal: to make sure that personally identifiable information is used in good rather than bad ways.

9. Give blue objects to half the groups. Explain that those groups will be on the Blue Team. They will record good, nice, and helpful ways to use personally identifiable information in the second column of *Personally Identifiable Information.*

Vocabulary Tips

In cybersecurity, the term *Blue Team* refers to professionals who defend and protect digital assets, while *Red Team* refers to professionals who try to break into digital systems and identify weaknesses that can be corrected. (Sometimes, the same individual serves on both teams.) Both mindsets are important to identify and fix ways that attackers could misuse information. Using these terms helps students become familiar with career options in cybersecurity.

Material Tips

Ensure that the objects representing teams can be distinguished in non-visual ways, such as by shape, size, or a label, so that blind or color-blind students can know which teams they are on.

10. Give red objects to half the groups. Explain that those groups will be on the Red Team. They will record bad, mean, and criminal ways to use personally identifiable information in the third column of *Personally Identifiable Information.*

11. Give students five minutes to brainstorm uses of personally identifiable information and record them in the appropriate column of *Personally Identifiable Information.*

12. After groups have brainstormed ideas, switch the objects so every group is now on the opposite team (Red or Blue). Give students five more minutes to brainstorm uses for personally identifiable information appropriate to their new team and record their ideas on *Personally Identifiable Information.*

13. Have students share the ideas they brainstormed. Ask:

> **Q: What good, nice, or helpful ways to use personally identifiable information did you brainstorm?**
>
> *A: Responses will vary. Possible responses include going to visit people, sending messages via mail, phone, email, or social media, playing games, watching videos, and buying things.*

Q: What bad, mean, or criminal ways to use information did you brainstorm?

A: Responses will vary. Possible responses include harassing people, stalking them, impersonating them, and stealing from them.

Q: If you were a cybersecurity professional, would you want to be on the Blue Team or the Red Team? Why?

A: Responses will vary. Possible responses include wanting to be on the Blue Team to protect people or wanting to be on the Red Team to figure out the puzzle of breaking into systems.

14. Have students consider both the benefits and drawbacks of sharing personally identifiable information by asking the following question:

Q: Is it better to share personally identifiable information or keep it private? Why?

A: Accept all responses. Students may consider how making personally identifiable information public allows people to use it for good purposes (for example, to contact their friends) but also for bad ones (for example, to bully others).

Material Tips

You can have students discuss questions 14 and 15 as a whole class, in small groups, or in pairs. Choose the best method for your students.

Introduce the idea of a **trade-off,** or a gain in terms of one factor with a simultaneous loss in terms of another factor. Perfect security is impossible, so protecting information always involves trade-offs (in cybersecurity, this concept is called *risk* acceptance). Explain that students have been thinking about trade-offs between the benefits and drawbacks of making personally identifiable information public.

15. Explain that while information can be stored in many ways, it is often stored on computers. The information that computers store and process is **data**. If a computer is connected to a network of other computers, the data it stores can potentially be accessed from those other computers. Ask:

Q: When we store personally identifiable information as data on a computer network, what are the trade-offs between benefits and risks?

A: Responses will vary. A possible response is that storing personally identifiable information as data on a computer network makes many tasks more convenient, such as contacting people, finding locations, and making purchases, but it can also make it easier for others to access the data when they are not supposed to.

16. Explain that in the next lesson, students will experiment with ways that attackers, or people who use the Internet to steal, hurt, or cause damage, can access and misuse personal data.

The Value of Information

Overview

Looking Back
In Lesson 1, students explored the concept of data and, more specifically, personally identifiable information and how it can be used in good and bad ways.

In This Lesson
Students act out a model of how information travels on the Internet, then use the model to explore how cyberattacks work.

Looking Ahead
In Lesson 3, students use their knowledge of cyberattacks to explore cybersecurity techniques, such as security awareness, antivirus software, encryption, and firewalls.

Guiding Question

How does information travel on the Internet, and how do cyberattacks take advantage of that process?

Objectives

Students will be able to

- demonstrate how information travels on the Internet.
- explore how cyberattacks exploit the Internet to cause damage.

Time

- 30 minutes

Grade Level: 6–8

Vocabulary

- **Computer**
- **Cyberattack**
- **Internet**
- **Model**
- **Network Device**
- **Protocol**
- **Request**
- **Response**
- **Server**
- **User**

Standards

CSTA 2-NI-04. Model the role of protocols in transmitting data across networks and the Internet.

Background

The Internet is a network of computer networks around the world. The Internet enables connections among many types of computers. In everyday speech, the word *computer* usually refers to desktop or laptop computers. However, any technology that gets input, stores and processes information, and gives output is a computer.

Different computers have different functions. Users interact with some computers (such as tablets, smartphones, smartwatches, televisions, and smart speakers). Servers process requests and provide services to users' computers. Network devices (such as routers) connect users' computers to each other

and to servers.

Users can connect to the Internet through a computer and request information, such as a webpage. Such requests travel through network devices on wireless networks (such as Wi-Fi and Bluetooth) and physical networks (such as wires and fiber optic cables), until they eventually arrive at the server that has the requested information. When a request reaches the appropriate server, the server processes the request and sends a response back to the user.

The speed and scale of the Internet enables many beneficial interactions, such as communication, buying and selling, and the sharing of information and opinions. However, it is also vulnerable to cyberattacks, which are ways of using the Internet to steal, hurt, or cause damage. Cyberattacks take advantage of weaknesses at various points within the Internet, including servers, network devices, users' computers, and users themselves.

The Internet is so big and complex that no one understands everything about it. You and your students can learn about it together.

Preparation

For the educator:

Part One

- A way to create and view a list as a class (e.g., whiteboard, chart paper, shared document)
- *Computer Images* (English | Spanish Coming Soon) for display

Part Two

8 index cards

- 1 copy of *Sample Requests and Responses* (English | Spanish Coming Soon), pages 1–4
  - Cut out requests #1–4 (front and back) and responses #1–4 (front and back) and tape or glue to index cards to create 8 sample cards (4 two-sided requests and 4 two-sided responses to those requests)
  - You do not need to cut out pages 5 and 6; you can print them as part of Sample Requests and Responses for student reference in Part 3.

For each student:

Part One

- 1 nametag (use *Address Nametags* (English | Spanish Coming Soon) or make your own) and a method to attach it to their clothing

- *Address Nametags* has 30 nametags. If you have fewer than 30 students, remove some nametags while keeping an equal number of Users, Servers, and Network Devices. Don't remove the Weather, Encyclopedia, Games, or Store Servers.

- 1 pencil

Part Three

- 1 blue object (to identify student as Blue Team)
- 10+ index cards or small pieces of paper
- 1 card cut from *User Information Cards* (English | Spanish Coming Soon)
- 1 copy of *Sample Requests and Responses* (English | Spanish Coming Soon) (optional)

Part Four

- additional index cards or small pieces of paper
- 1 red object (enough for half the students; the other half will keep using blue objects)
- 1 copy of *Red Team Suggestions* (English | Spanish Coming Soon)

EiE® Connections

Learn more about the Engineering Design Process in the EiE Video Library.

Continue your classroom activities with these units:

Computer Science Essentials™

- *Building Automated Systems*
- *Designing Computer Games*
- *Analyzing Digital Images*

Note that the Computer Science Essentials™ series is part of Engineering and Computer Science Essentials™: An Integrated Program.

Museum of Science Connections

Explore the interactive infographic "Defending the Internet."

Listen to the Pulsar podcast episode "What Is Data?" (10 minutes)

Watch the conversation *A Reno Family Foundation Symposium: Cyberattacks & Information Terrorism: The Next World War?* (1 hour 30 minutes)

Family Connections

Continue the learning at home with this activity:

- Careers for Engineers Quiz

Credits

This lesson is offered at no cost thanks to the generosity of the Akamai Foundation.

Activity Instructions

This activity has four parts.

- The purpose of **Part One** is for students to learn about parts of the Internet. Students create a live-action model of these elements. Some students represent Users, some represent Servers, and some represent the Network Devices connecting them.

- The purpose of **Part Two** is for students to learn how information travels on the Internet. They act out worked examples of requests going from Users to Servers and responses going from Servers to Users. Requests and responses are represented by index cards.

- The purpose of **Part Three** is for students to explore the flow of information on the Internet in an open-ended way. They do this by acting out the process in Part Two but with the added freedom of choosing which requests and responses to send. In this part, everyone is on the Blue Team and using the Internet model for good purposes.

- The purpose of **Part Four** is for students to learn about cyberattacks. To do this, some students are switched to the Red Team. The class acts out the process from Part Three, but Red Team students now attempt to find weaknesses by stealing or altering personally identifiable information, interfering with the movement of index cards, and generally causing damage.

You can conduct all parts of the activity in a single class session or split them up over two sessions. If you split them up, conduct Parts 1 and 2 in the first session and Parts 3 and 4 in the second session.

Part One: Parts of the Internet

1. Remind students about their previous exploration of data, particularly personally identifiable information, and ways it can be used and misused. Explain that today, students will think about information when it exists as data on computers that are connected to the Internet. Review students' answers to the question **What is the Internet?** from the beginning of Lesson 1. Allow them to add ideas.

2. Synthesize and build on student responses to ensure they understand the Internet is a network of computer networks around the world. Display and describe the pictures of computers for users on slide 1 of *Computer Images* (English | Spanish Coming Soon) to provide examples.

Vocabulary Tips

If necessary, explain that a computer is a technology that gets input, stores and processes information, and gives output. Any technology that can access the Internet, such as a smartphone, television, smart speaker, or smartwatch, is a computer.

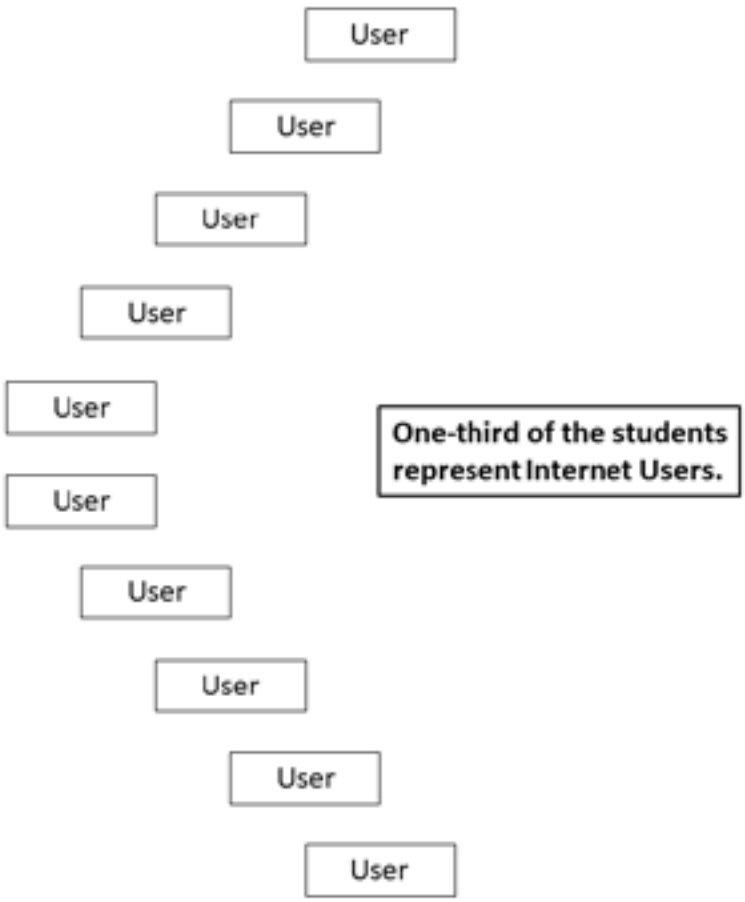
3. Explain that today, students will create a **model** of the Internet. If necessary, explain that a model is a representation of an object, system, or process. Whereas the real Internet is composed of computers and data, students will model the Internet using people and paper.

Activity Tips

If your students have experience creating or using models in science, activate their prior knowledge by showing or describing some of the work they did or phenomena they studied.

4. Using students' prior knowledge about the Internet as a guide, explain that Users are one element the class will model. If necessary, explain that a **user** is a person who accesses the Internet.

5. Assign (or get volunteers from) one-third of the students to represent Internet Users. Give each a "User" nametag, a pencil, and a stack of index cards. Have each User write their name on the nametag.

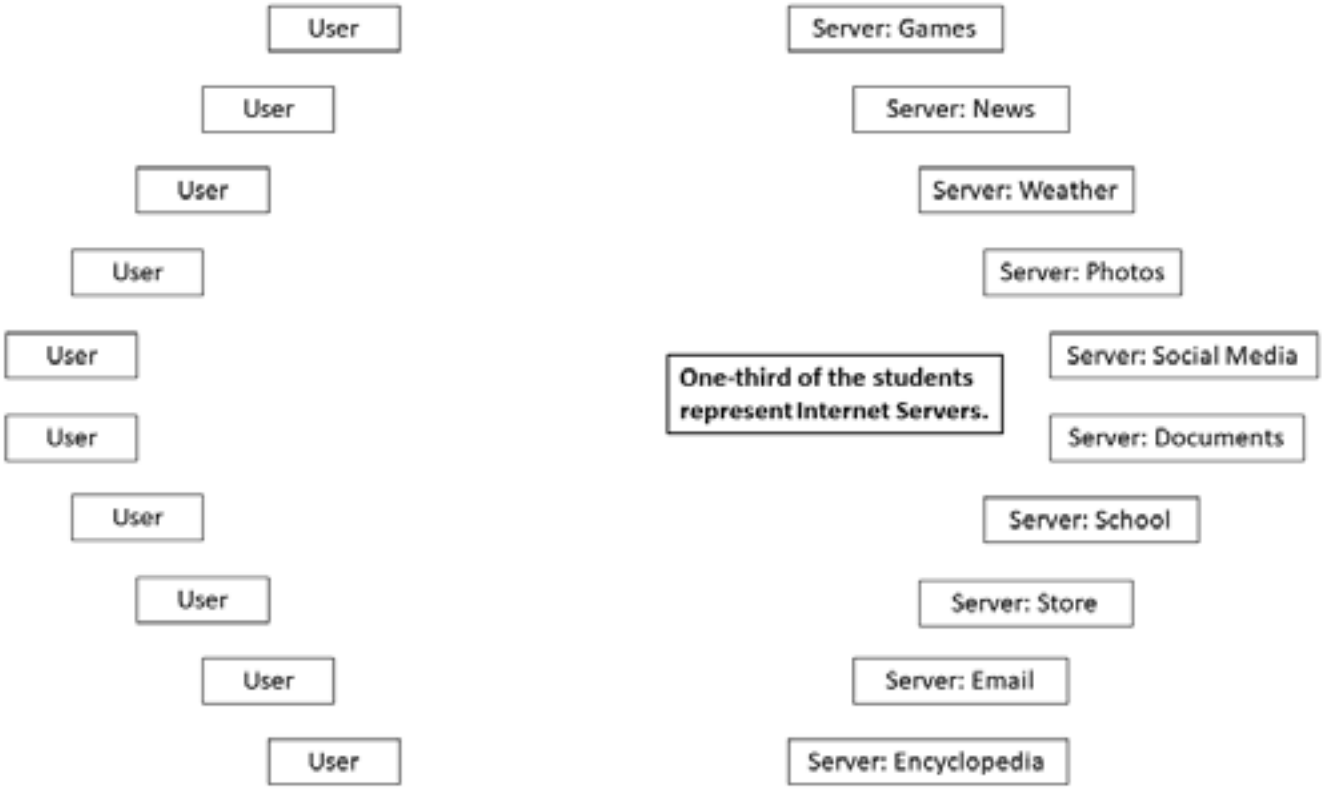


Activity Tips

If your students have experience creating or using models in science, activate their prior knowledge by showing or describing some of the work they did or phenomena they studied.

6. Explain that a **server** is a computer with software that processes requests or provides a service to users. For example, users access webpages by making requests to servers. Display and describe the pictures of servers on slide 2 of *Computer Images* (English | Spanish Coming Soon) to provide examples. Explain that server software usually runs on specially designed computers, but any computer with good enough hardware can act as a server.

7. Assign (or get volunteers from) one-third of the students to represent Internet Servers. Give each a "Server" nametag, a pencil, and a stack of index cards. Point out that each "Server" nametag is associated with a particular type of website



Activity Tips

To make the model easy to understand, consider having all students representing Servers gather on the side of the room opposite the students representing Users.

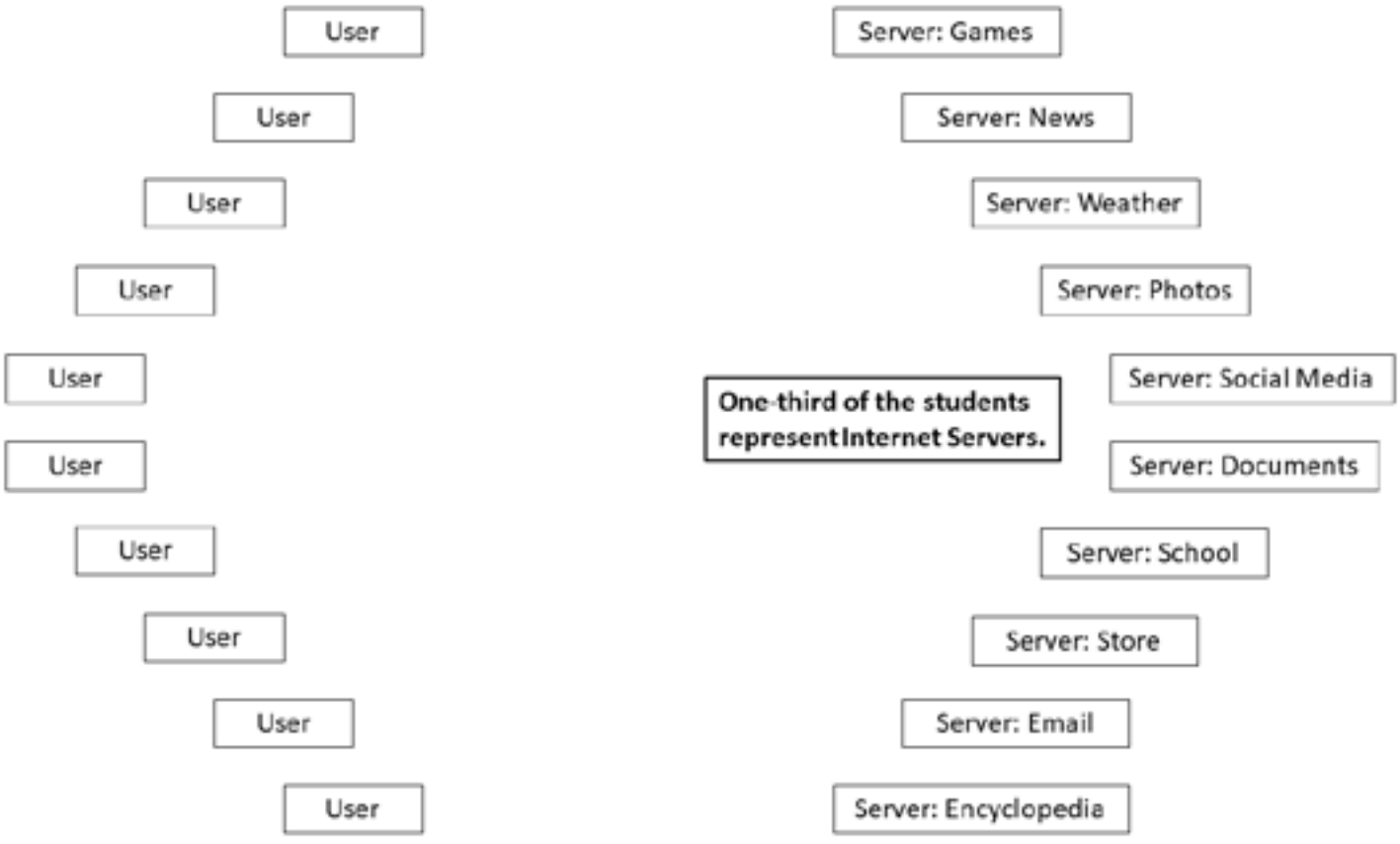
If appropriate, students can choose to represent specific websites rather than the general categories provided on Address Nametags. For example, the student with the "Social Media" nametag can choose a specific social media site to represent. You may also let students create server types not represented on the pre-made nametags (such as "Maps").

8. Finally, draw on students' prior knowledge about the Internet to explain that the class will model network devices connecting users and servers. Explain that a **network device** is a computer or other technology that helps connect users' computers each other and to servers. Display the pictures of network devices on slide 3 of *Computer Images* (English | Spanish Coming Soon) to provide examples.

Activity Tips

To illustrate how network devices are connected, look up a live cybersecurity threat map online. These maps illustrate the structure of network connections across the Internet by showing in-progress cyberattacks.

9. Assign the remaining one-third of the students to represent the Network Devices that carry data between Users and Servers. Give each a "Network Device" nametag.



Activity Tips

To make the model easy to understand, consider having all students representing Network Devices gather at the center of the classroom, between the students representing Users and the students representing Servers.

10. To make sure students know their roles, give the following instructions:

- **If you are a User, raise your hand.**
- **If you are a Server, raise your hand.**
- **If you connect Users and Servers, raise your hand.**

Part Two: How Information Travels on the Internet

1. Ask:

> **Q: What do you do to go to a website?**
>
> *A: Responses will vary. Possible response: enter an address or click on a link or icon.*

2. Explain that students have just described a **request**. A request is a message from a computer to a server asking for information. Requests are sent following a **protocol**, or a set of rules for computers to send and receive information. For example, the protocol can require that every request includes the name of the sender, the name of the server it is being sent to, and the specific information requested.
3. Tell students that, although requests on the actual Internet are submitted by doing things such as entering website addresses and clicking links and icons, they will submit requests in their model using index cards.

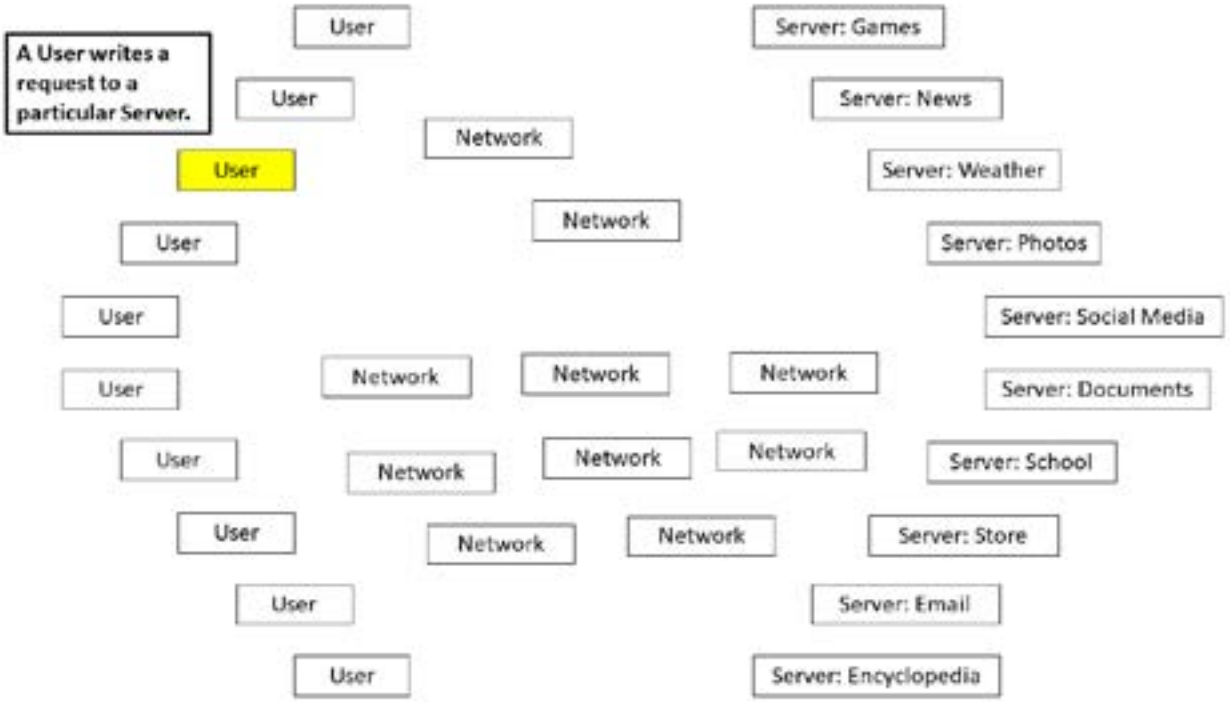
- The front of an index card will say who it is coming from and going to, while the back will have a request or response.
- **Users** will write out requests and give them to **Network Devices.**
- **Network Devices** will deliver them to **Servers.**

As an example, display and read Sample Request #1 in *Sample Requests and Responses* (English | Spanish Coming Soon).

Sample Request #1 From: To: Weather	Sample Request #1 What will the weather be tomorrow?

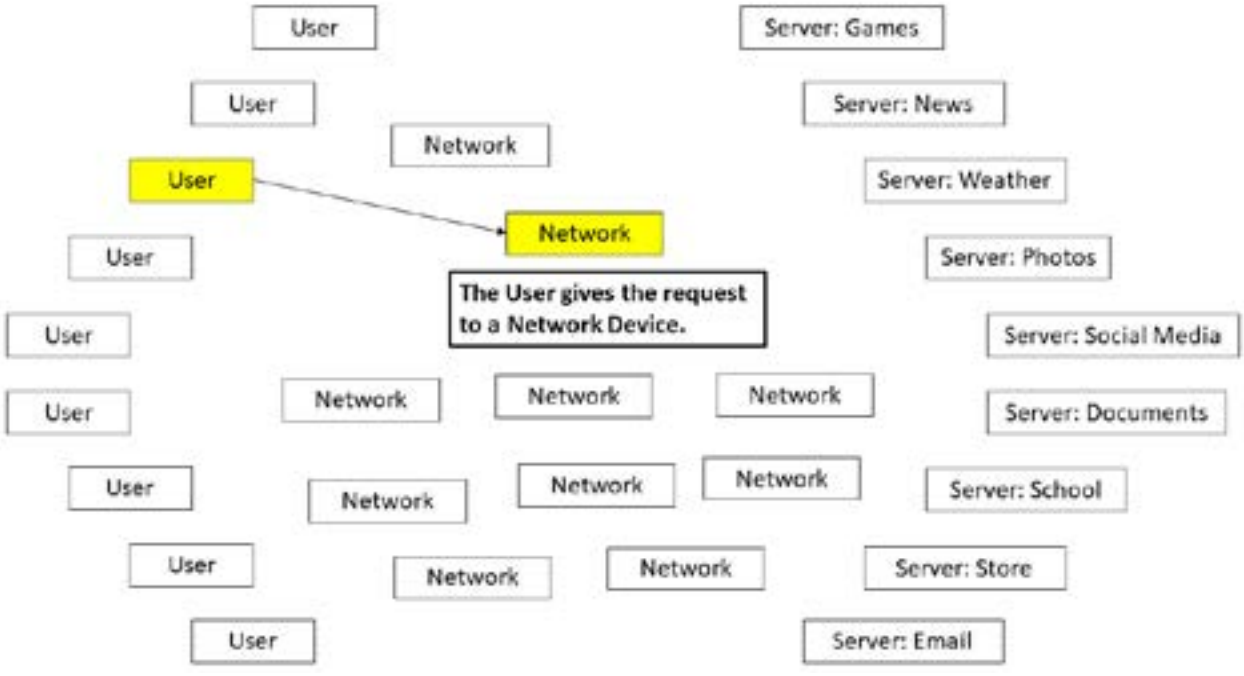
4. Give the Sample Request #1 card to a User student. Have them write in their name. The address and message are already written for them. Say:

First, a User writes a request to a particular Server.



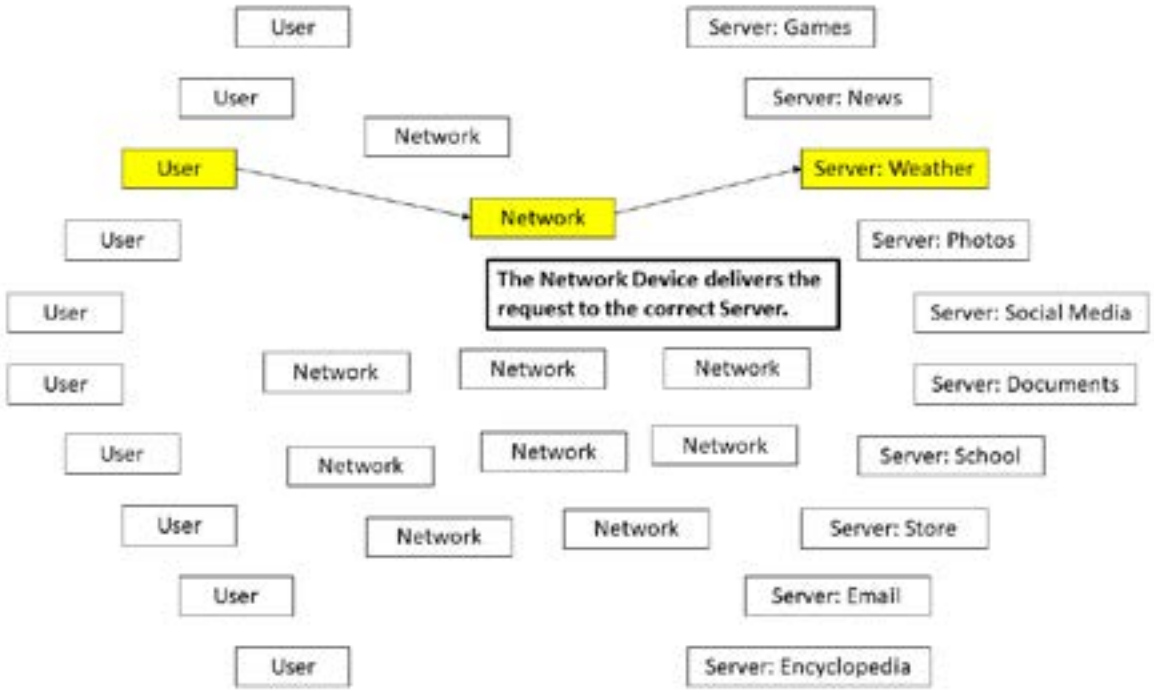
5. Explain that once a User has written a request, they give it to a Network Device. Have the User you chose call over a Network Device and give them the request. Say:

Next, the User gives the request to a Network Device.



6. Explain that the Network Device delivers the request to the correct Server. Have the Network Device with the request deliver it to the Weather Server. Say:

Then the Network Device delivers the request to the correct Server.



Activity Tips

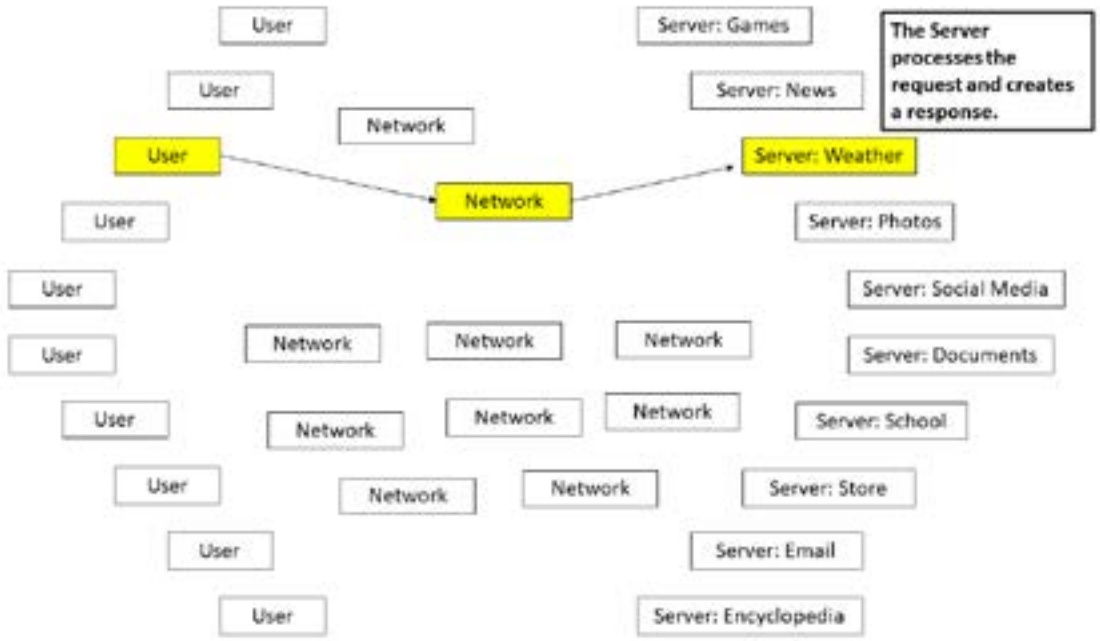
On the actual Internet, requests and responses pass through many different network devices on their way between users and servers. To make the model more accurate, you can have Network Devices give index cards to each other before giving them to Servers (or back to Users). However, this process adds complexity and may slow down the model. Choose the option that is right for your class.

7. Explain that the Server processes the request and then creates a response. Tell students that a **response** is a message from a server back to another computer as an answer to a request. Like a request, a response is also sent following a **protocol**. Every response will include the name of the server, the name of the user it is being sent to, and the specific information requested. As an example, display and read Sample Response #1 in *Sample Requests and Responses* (English | Spanish Coming Soon).

Sample Response #1 From: Weather To:	Sample Response #1 The sun will be shining tomorrow.

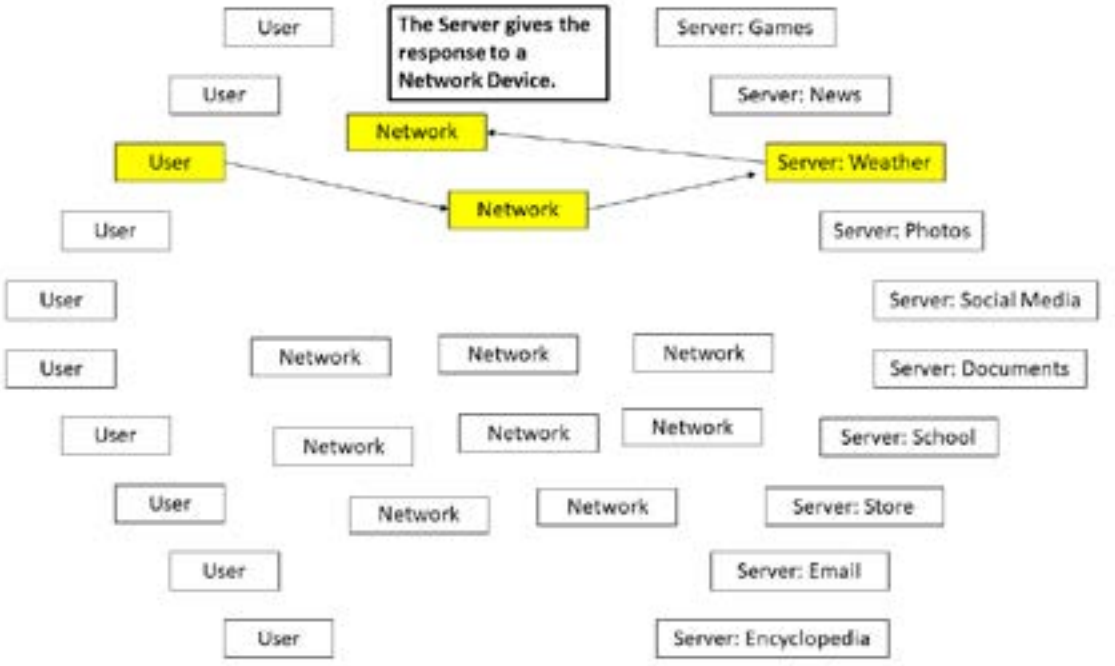
8. Give the Sample Response #1 card to the Weather Server. Have them write in the name of the User who made the request. The Server address and message are already written for them. Say:

The Server processes the request and creates a response.



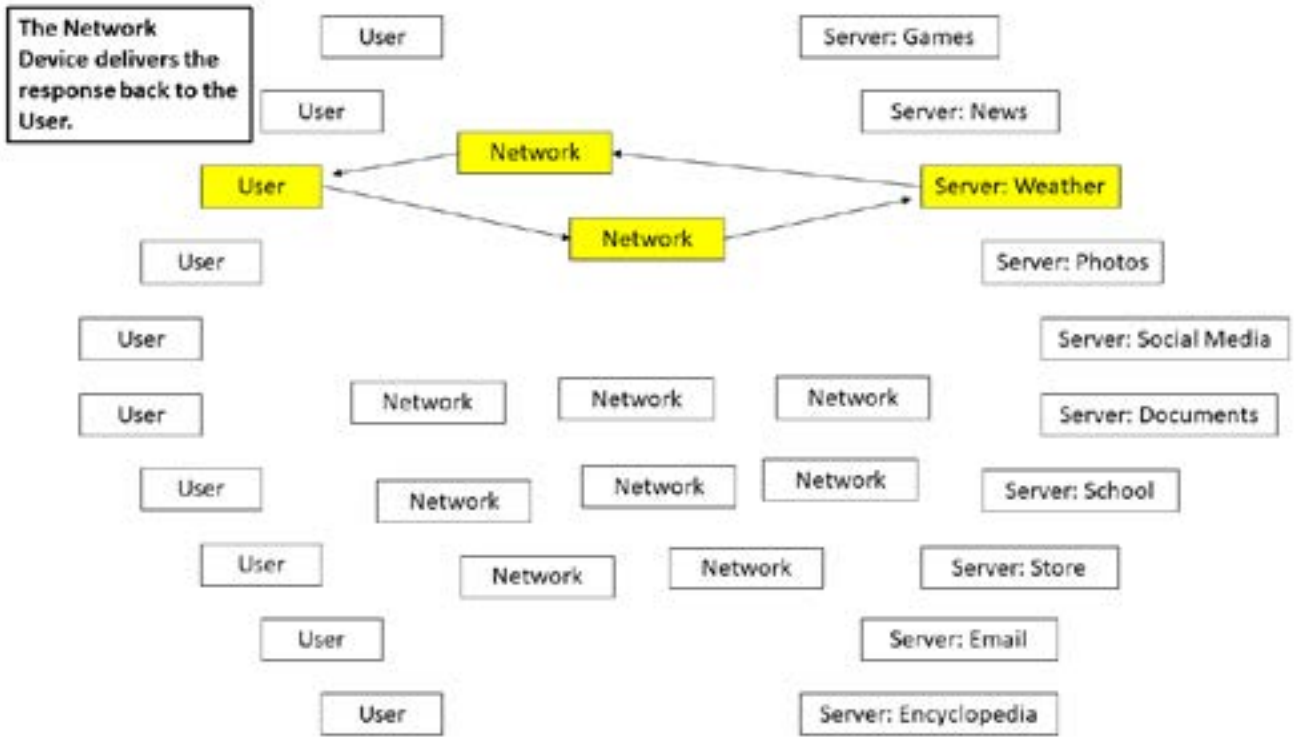
9. Explain that once the Server has written the response, they give it to a Network Device. Have the Weather Server call over a Network Device and give them the response. (It does not need to be the same Network Device that carried the request.) Say:

10. **Next, the Server gives the response to a Network Device.**



11. Explain that finally, the Network Device delivers the response to the User who sent the request. Have the Network Device with the response deliver it to the original User. Say:

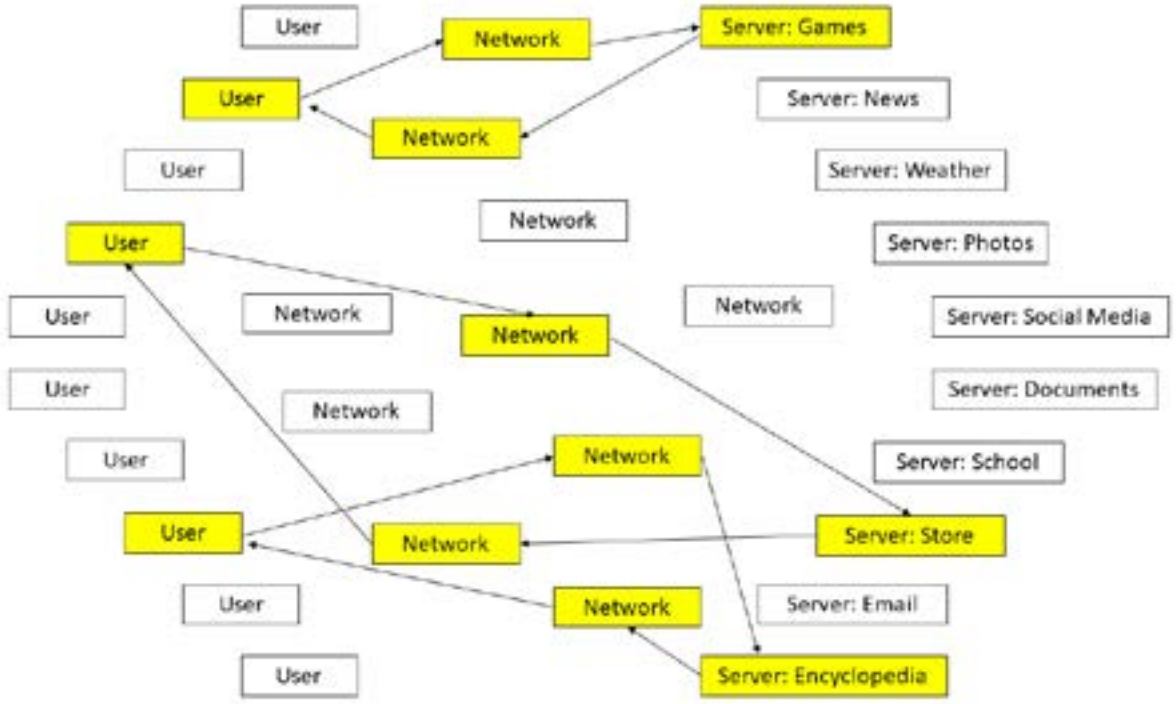
Finally, the Network Device delivers the response back to the User.



12. Check for understanding by asking the following question:

> **Q: What are the steps in the request-response process?**
>
> *A: A User writes a request and gives it to a Network Device. The Network Device delivers it to the correct Server (or to another Network Device). The Server reads the request and writes a response. The Server gives the response to a Network Device. The Network Device delivers the response to the original User (or to another Network Device).*

13. Once students understand the process, demonstrate how multiple requests and responses can be sent at once. Give Sample Requests #2, 3, and 4 to three Users and Sample Responses #2, 3, and 4 to the Encyclopedia, Games, and Store Servers, respectively. Have all three Users send their requests at the same time and have everyone represent the request-response process.



Part Three: Open-Ended Exploration

1. Now that students understand how the Internet model works, explain that they will explore it in an open-ended way. Users can write (respectful and appropriate) messages to whichever Servers they want. They will give the messages to Network Devices to carry to those Servers. The Servers will write responses and give them to Network Devices to carry back.

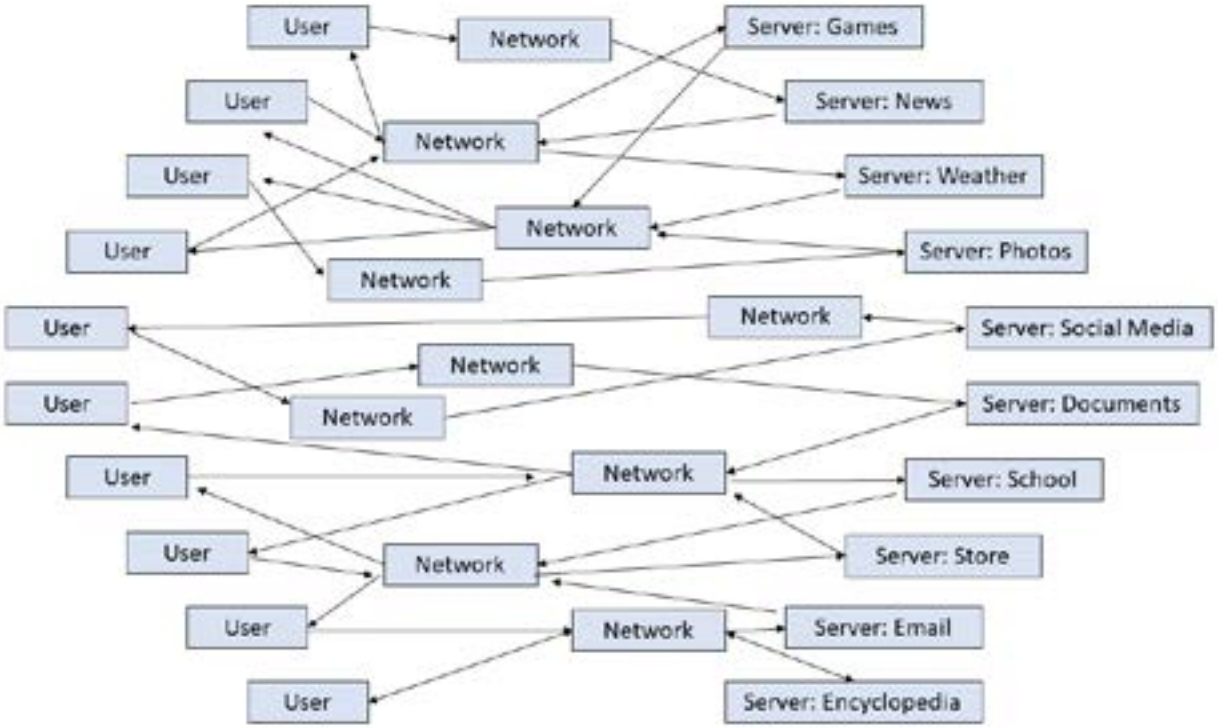
2. Since writing on and reading index cards may not be accessible or engaging for all students, introduce alternatives as appropriate for your class. For example, you might have Network Devices record audio or video requests and responses on phones and then play them for recipients.

3. Give every User a card cut from *User Information Cards* (English | Spanish Coming Soon). Explain that these cards contain made-up personally identifiable information such as account names and passwords that Users may need to send in their requests.

4. Give every student a blue object. Explain that for now, everyone is on the Blue Team and is using the Internet for good, kind, and helpful purposes.

5. You can provide every student with a copy of *Sample Requests and Responses* (English | Spanish Coming Soon) to give them ideas.

6. Run the model for several minutes.



Activity Tips

If a User composes a long request or a Server creates a long response that requires multiple index cards, note that this phenomenon reflects the structure of the Internet, in which messages are divided into small, separately transmitted "packets."

7. Every few minutes, have students switch roles so that every student can experience representing a User, a Network Device, and a Server. Remember to have students switch nametags when they switch roles. New Users should put their names on their User nametags. Give a new card from *User Information Cards* (English | Spanish Coming Soon) to each new User. Give out additional index cards as necessary.

8. Check for understanding by asking the following question:

Q: What are some ways you used the Internet in this model?

A: Accept all responses. Possible responses include sending and receiving information, making social connections, and being entertained. All responses should describe the roles of Users, Network Devices, and Servers in the request-response process.

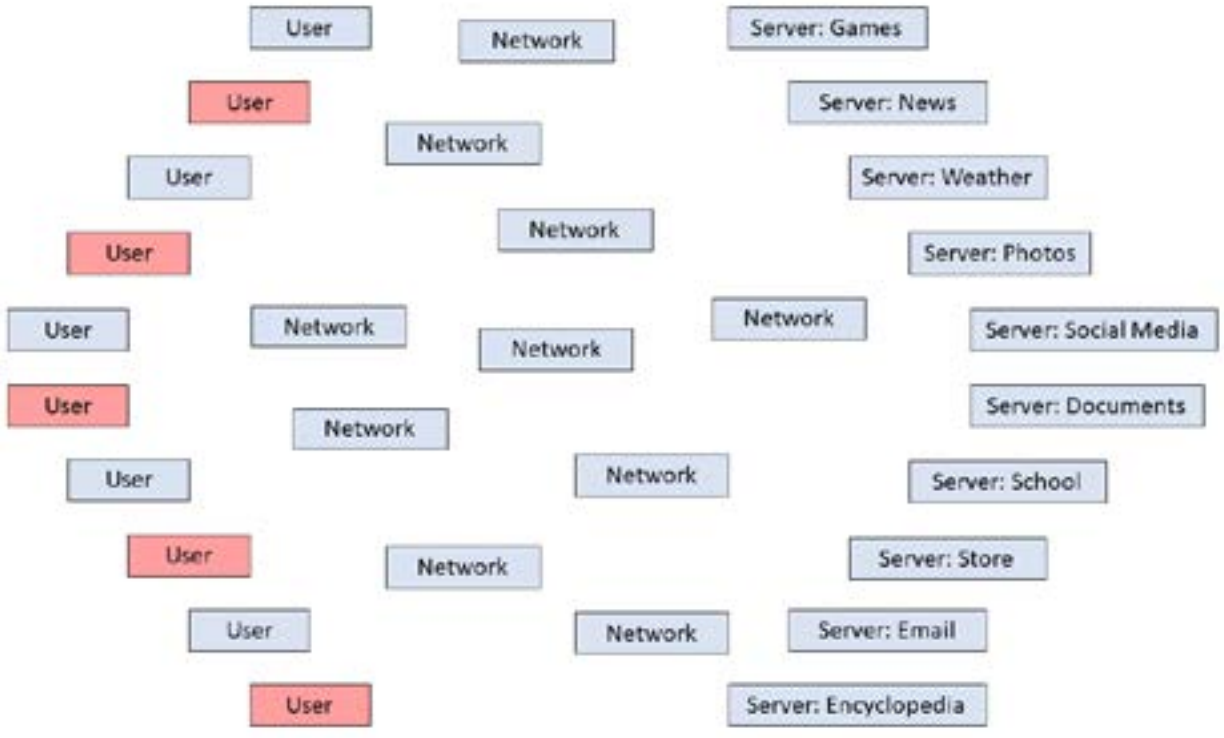
Part Four: How Cyberattacks Work

1. Explain that unlike in the model students have used so far, not everyone on the real Internet is trying to do good. Ask:

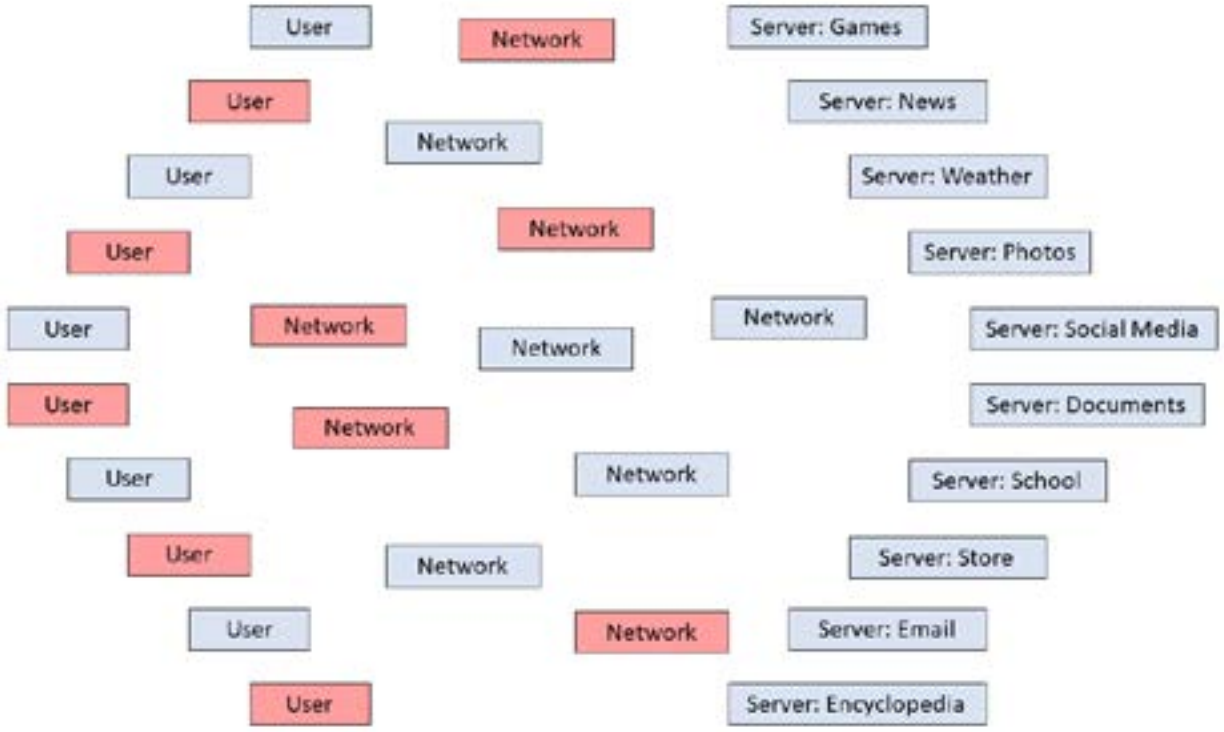
> **Q: When we thought about personally identifiable information, what bad, mean, or criminal ways did we think of for people to use it?**
>
> *A: Responses will vary. Possible responses include harassing people, stalking them, impersonating them, and stealing from them.*

Explain that attackers use the Internet to get personally identifiable information and do these kinds of things.

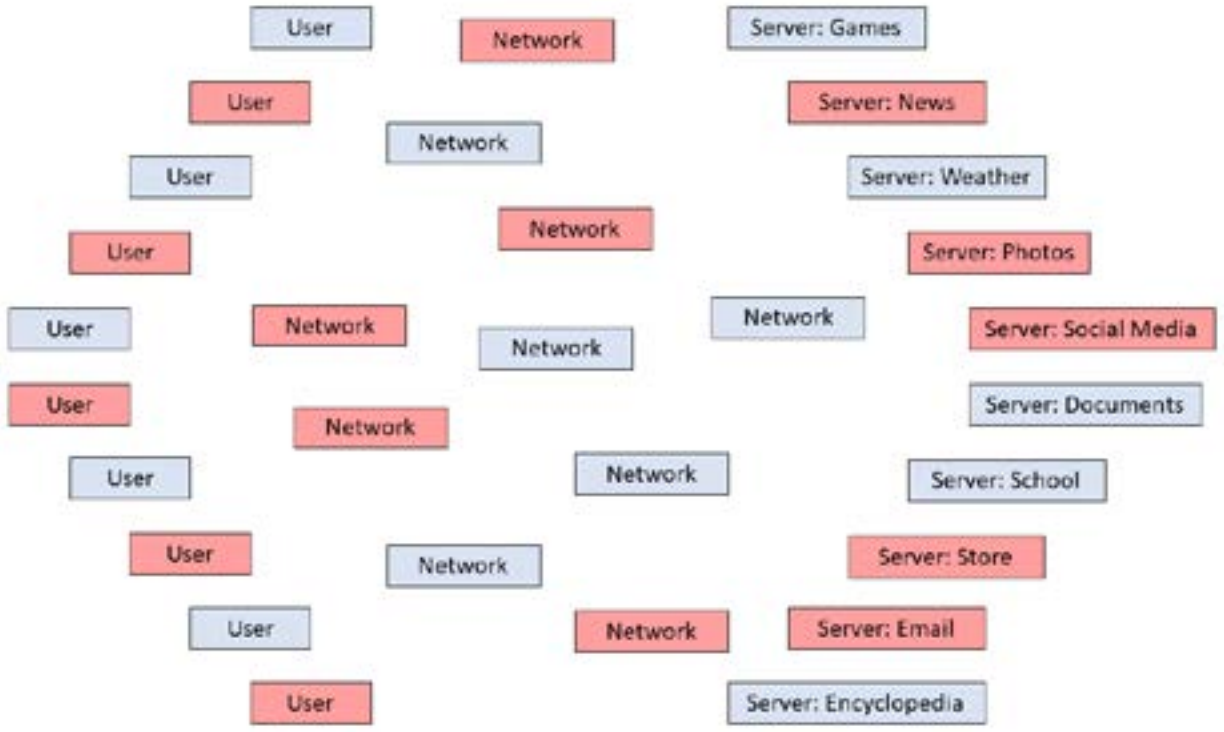
2. Switch the objects of half the Users from blue to red to represent that they are on the Red Team. Explain that these students will now represent cybersecurity professionals who try to find weaknesses in the system students are modeling.



3. Switch the objects of half the Network Devices from blue to red to represent that they are now on the Red Team. Explain that these students will now represent Network Devices under the control of Red Team professionals.



4. Switch the objects of half the Servers from blue to red to represent that they are now on the Red Team. Explain that these students will now represent Servers under the control of Red Team professionals.



5. Bring together all the Red Team students and give each a copy of *Red Team Suggestions* (English | Spanish Coming Soon). Explain that

- this sheet has suggestions for ways in which they can steal personally identifiable information and cause problems.
- they cannot physically interfere with other students—for example, by grabbing, hitting, or tackling them.
- they must follow the protocols they have already practiced and can interfere only through the ways in which they create and handle requests and responses.

6. If time permits, allow all Red Team students to brainstorm together as a group. Allow Blue Team students to brainstorm other ways in which to use the Internet model.

7. Hand out more index cards if necessary.

8. Run the model again. Observe and take note of the ways in which Red Team students intervene or interfere in the request-response process. As necessary, remind students to refrain from physically interfering with each other.

9. After the model has run for several minutes, have every member of the Blue Team switch their object with a member of the Red Team. Give copies of *Red Team Suggestions* (English | Spanish Coming Soon) to the new Red Team members and give them a few minutes to strategize. Then run the model again.

Activity Tips

As time and interest permit, you can also have students change roles among Users, Network Devices, and Servers.

10. Once everyone has had a chance to participate on both teams, pause the model. Ask:

> **Q: What were some of the things the Red Team did?**
>
> *A: Accept all responses. Possible responses include lying to get information, sending viruses, altering requests or responses or failing to deliver them, and overloading servers with messages.*

Record students' answers on a whiteboard, chart paper, or some other medium for later reference. Explain that the techniques used by the Red Team are like those used by attackers on the actual Internet.

11. Explain that *phishing* refers to sending a message to trick a user into revealing personally identifiable information or downloading malware. Phishing is a form of social engineering, which refers to tricking people into revealing personally identifiable information. Ask:

Vocabulary Tips

Although phishing usually refers to malicious email messages, it can also refer to malicious messages sent in other ways, such as through texts or voicemail.

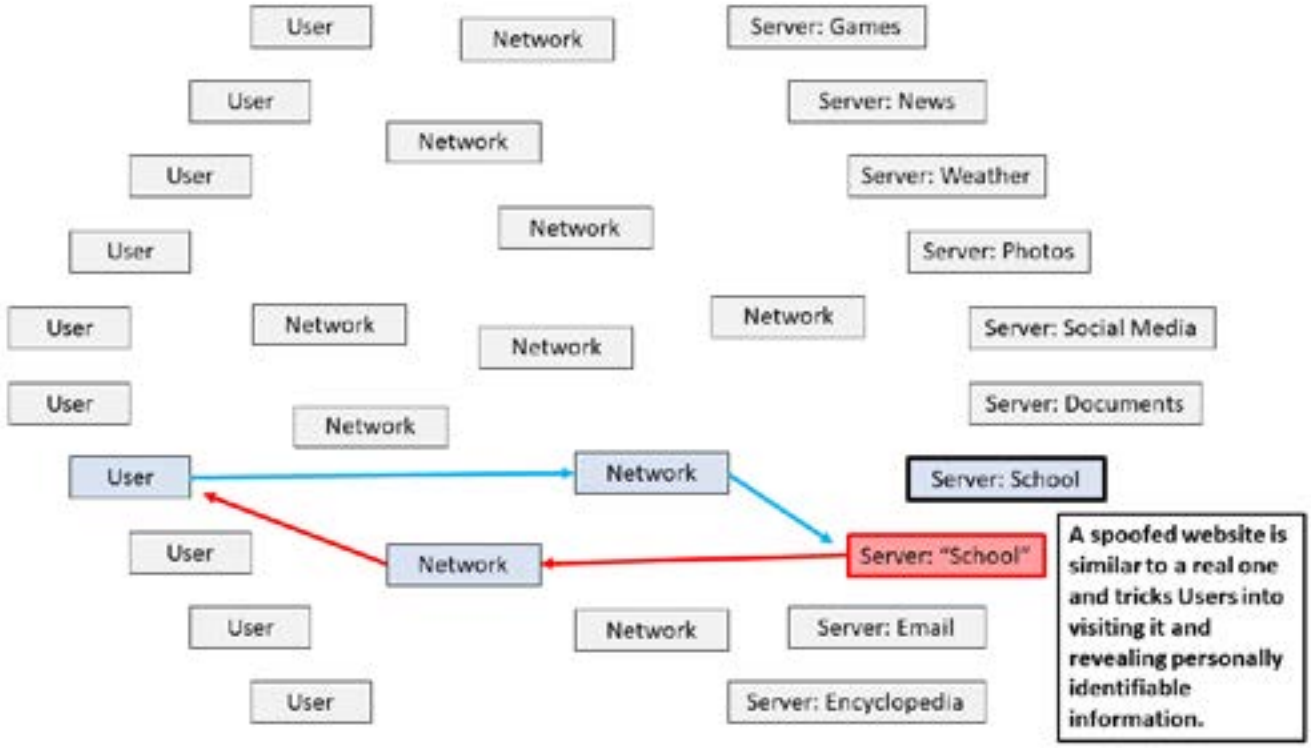
Q: Did anyone on the Red Team use phishing? How?

A: Responses will vary. Possible responses include sending a message pretending to be someone else or asking for personally identifiable information as part of a game, survey, or contest.

Have the class consider whether the things the Red Team members did were in fact examples of phishing.

Response Take a survey to win 100 GameBuck$! Enter your password to begin.	Response Your School password needs updating. Enter your current School password to continue.

One method of phishing is *website spoofing*, which refers to hackers setting up a fake version of a real website with a similar design and address to trick people into entering personally identifiable information. The Red Team may have modelled this behavior by creating a new Server nametag with a name similar or identical to another Server.



Ask:

Q: Did anyone manage to get personally identifiable information while they were on the Red Team?

A: Responses will vary. Red Team students may have tricked Blue Team students into revealing information from their User Information Cards.

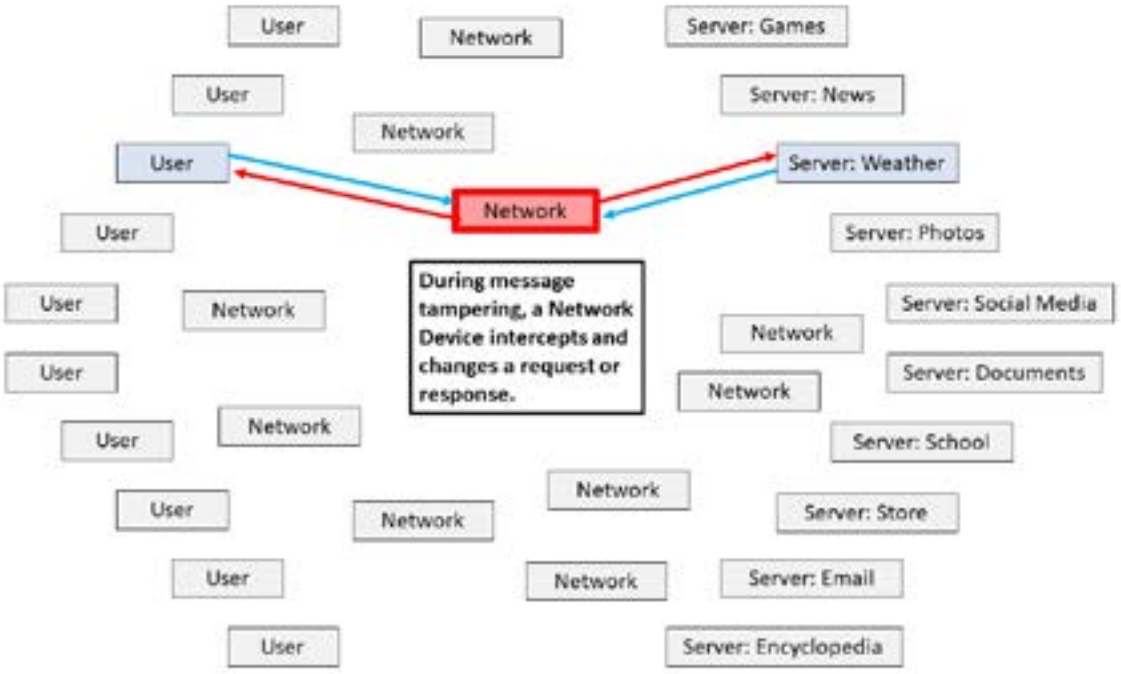
Q: How could the Red Team use personally identifiable information that they gathered?

A: Responses will vary. The Red Team could use someone's personally identifiable information to impersonate that individual. The Red Team could also use personally identifiable information to guess passwords. For example, someone's password could be their birthdate or home address. Once a member of the Red Team learns one password, if the user has that same password for multiple accounts, the member of the Red Team can break into all those accounts.

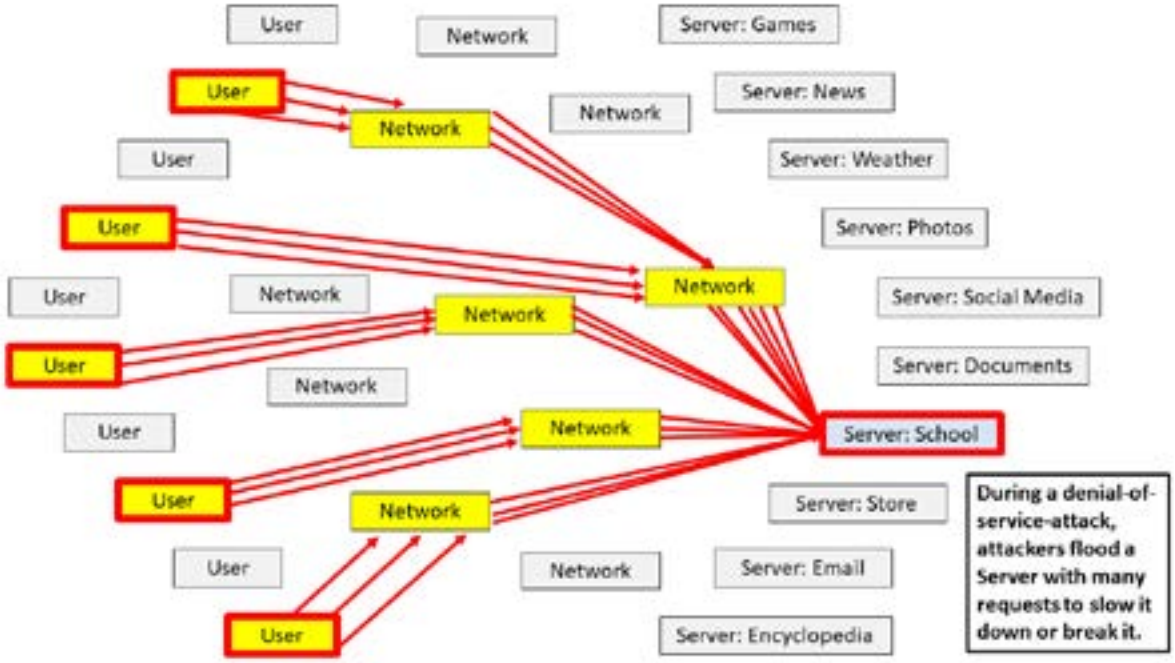
12. Explain that malware refers to downloaded software that steals information from a computer or lets an attacker infect the computer with remote-control software. Red Team Users or Servers may have modelled this behavior by sending index cards with the word virus or a similar message or image on the back.

Response From: Store To:	This is a virus download. Show your personally identifiable information to this Network Device. You are on the Red Team now.

13. Explain that *eavesdropping* refers to intercepting and reading requests or responses, while message tampering refers to intercepting and changing requests or responses. Red Team Network Devices may have modelled this behavior by reading or changing the messages on index cards.



14. Explain that a *denial-of-service attack* refers to sending many requests to a Server or other part of a network to slow it down or break it. Red Team Users may have modelled this behavior by sending many requests to a single Server. (In real life, attackers can infect ordinary people's computers and use those computers to send the requests.)



15. Tell students that all these behaviors are examples of cyberattacks—uses of the Internet to steal, hurt, or cause damage. Such attacks happen against organizations and individuals. Ask:

> **Q: Have you or people you know ever gotten a phishing message? What did it say?**
>
> *A: Responses will vary. Students may share examples of suspicious emails, text messages, or voicemails asking for personally identifiable information.*

> **Q: Have you or people you know ever experienced other forms of cyberattack? What were they?**
>
> *A: Responses will vary. Students may have had an organization, such as their school, disrupted by a cyberattack. The attack may have involved ransomware, a type of malware that prevents users from accessing their data until they pay money.*

16. Explain that next time, students will explore ways to protect themselves, their classmates, their families, and their communities from cyberattacks.

The Value of Information

Overview

Looking Back
In Lesson 1, students learned about personally identifiable information and its value. In Lesson 2, they thought about how such information is shared on the Internet and how it can be compromised by cyberattacks.

In This Lesson
Students explore methods to protect information from cyberattacks, consider ways to keep themselves and others safe online, and learn about cybersecurity careers.

Guiding Question

How can we keep our personally identifiable information safe?

Objectives

Students will be able to

- develop practices to protect their information and themselves online.
- explain how cybersecurity practices prevent cyberattacks.

Time

- 30 minutes

Grade Level: 6–8

Vocabulary

- **Antivirus Software**
- **Authentication**
- **Cybersecurity**
- **Encryption**
- **Firewall**
- **Security Awareness**

Standards

CSTA 2-NI-05. Explain how physical and digital security measures protect electronic information.

CCSS.ELA-LITERACY.L.6–8.4.B. Use common, grade-appropriate Greek or Latin affixes and roots as clues to the meaning of a word.

Background

Cybersecurity is the protection of computers, data, and identity. Cybersecurity practices take many forms, such as physical (for example, locking computers in safe places), technical (for example, encrypting data), and behavioral (for example, not opening suspicious emails).

Cybersecurity practices are necessary throughout the Internet. Users can practice security awareness by providing personally identifiable information only when necessary and only to trustworthy entities. They can use antivirus software to prevent the loss of data or control to malware. They can encrypt data, meaning they change it to a form that unauthorized parties cannot understand. And they can secure servers and other parts of a network with firewalls that prevent the entry of suspicious or unauthorized requests.

There are many careers in cybersecurity. Defensive "Blue Team" careers focus on designing ways to protect computer systems (security engineering), helping when cyberattacks occur (security operations), and analyzing attacks to prevent their recurrence (digital forensics). Offensive "Red Team" careers focus on breaking into computer networks to determine where they have weaknesses and how they can be better secured. Some terms for Red Team careers include *ethical hacking, penetration testing, security assessment, vulnerability scanning, and white-hat hacking.*

Materials

For the educator:

Part One

- A way to create and view a list as a class (e.g., whiteboard, chart paper, shared document)

Part Two

- The video *Cybersecurity: Working with Puzzles* (3:40) (English | Spanish Coming Soon)
- A way to show the video to students

For each student:

Part One

- 1 copy of *Cyberattacks and Cybersecurity* (English | Spanish Coming Soon | Answer Key)
- 1 pencil

Part Two

- 1 object (blue for half the students, red for the other half)
- 1 nametag (you can use the nametags in *Address Nametags* (English | Spanish Coming Soon) or make your own) and a method to attach it (from Lesson 2)
- 10+ index cards or small pieces of paper
- 1+ envelopes (optional)
- 1 card cut from *User Information Cards* (English | Spanish Coming Soon) (from Lesson 2)
- 1 copy of *Red Team Suggestions* (English | Spanish Coming Soon) (from Lesson 2, for half the students)
- 1 copy of *Blue Team Suggestions* (English | Spanish Coming Soon) (for half the students)
- 1 copy of *Cybersecurity Reference* (English | Spanish Coming Soon)

Extension

- additional index cards or small pieces of paper
- 1 copy of *Transposition Ciphers* (English | Spanish Coming Soon)
- 1 copy of *Substitution Ciphers* (English | Spanish Coming Soon)

EiE® Connections

Learn more about the Engineering Design Process in the EiE Video Library.

Continue your classroom activities with these units:

Computer Science Essentials™

- *Building Automated Systems*
- *Designing Computer Games*
- *Analyzing Digital Images*

Note that the Computer Science Essentials™ series is part of Engineering and Computer Science Essentials™: An Integrated Program.

Museum of Science Connections

Explore the interactive infographic "Defending the Internet."

Listen to the Pulsar podcast episode "What Is Data?" (10 minutes)

Family Connections

Continue the learning at home with this activity:

Careers for Engineers Quiz

Credits

This lesson is offered at no cost thanks to the generosity of the Akamai Foundation.

Activity Instructions

This activity has two parts and one optional extension.

- *The purpose of* **Part One** *is for students to review basic kinds of cyberattacks and brainstorm possible ways to prevent them. They do this by completing a worksheet in small groups.*
- *The purpose of* **Part Two** *is for students to explore cybersecurity techniques in an open-ended way. They do this by acting out the Internet model from Lesson Two and using the cybersecurity techniques they brainstormed.*
- *The purpose of the* **Extension** *is for students to explore the cybersecurity technique of encryption. They do this by learning several simple encryption techniques, then applying them to encrypt requests and responses in their Internet model.*

Part One: Introduction to Cybersecurity

1. Remind students about their previous exploration of personally identifiable information, the flow of data on the Internet, and the concept of cyberattacks. Explain that today, they will think about ways to prevent cyberattacks.

2. Organize students (or have them organize themselves) into small groups. Give each student a copy of *Cyberattacks and Cybersecurity* (English | Spanish Coming Soon). Explain that they will work with their groups to

   - draw the flow of information during a cyberattack.
   - think of a way to prevent that kind of cyberattack in the class model.

Activity Tips

If time is limited, give each group only one page from Cyberattacks and Cybersecurity and have them share their thoughts with other groups. Otherwise, have each group complete all four pages.

3. Give groups 5–10 minutes to complete *Cyberattacks and Cybersecurity* (English | Spanish Coming Soon).

4. Check for understanding by asking the following question:

Q: What ideas did you come up with to prevent cyberattacks in our Internet model?

A: Responses will vary. Possible responses include not responding to suspicious messages, giving messages to people to check for viruses, folding up index cards or putting them in envelopes, and having Servers refuse to accept multiple requests at once.

Activity Tips

If it is helpful for student understanding, you can have groups act out different kinds of cyberattacks and ways to prevent them.

Record students' ideas on chart paper, a whiteboard, or in some other medium for the whole class to reference.

5. Explain that students have suggested techniques for **cybersecurity**, the protection of computers, data, and identity. As appropriate, share the real-world terms for the techniques students brainstormed:

- **Security awareness** means being careful when using the Internet—for example, by not replying to suspicious messages.
- **Antivirus software** is a computer program that checks for suspicious software and remote-control programs and stops them from working. It can be installed by a user or an associated group, such as their family or school.
- **Encryption** is changing data into a form that unauthorized parties cannot understand. Users normally don't need to think about it, but it is critical for keeping information private on the Internet.
- A **firewall** is a technology that lets only certain requests reach a server or other part of a network.

Activity Tips

Students may brainstorm a technique not listed here, and that's okay. It is probably similar to a real-world cybersecurity practice, even if you don't know the word for it. What matters is not specific vocabulary but helping students understand that there are ways to protect information on the Internet.

Activity Tips

As a real-world example of encryption, tell students that Hypertext Transfer Protocol Secure (HTTPS) protects data sent between websites and is therefore more secure than Hypertext Transfer Protocol (HTTP), an older method of sending information. Students can recognize websites that use the secure protocol because their addresses begin with "https." Preferring such websites to unsecured ones is a cybersecurity practice students can easily use.

If you have time after Part Two, implement the Encryption Extension Activity so students can explore encryption methods.

Part Two: Cybersecurity Exploration

1. Tell students they will use their Internet model to test the cybersecurity techniques they brainstormed against the cyberattacks from the previous lesson. Explain that

- the Red Team will represent cybersecurity professionals testing for weaknesses.
- the Blue Team will represent cybersecurity professionals finding ways to keep computer systems secure.

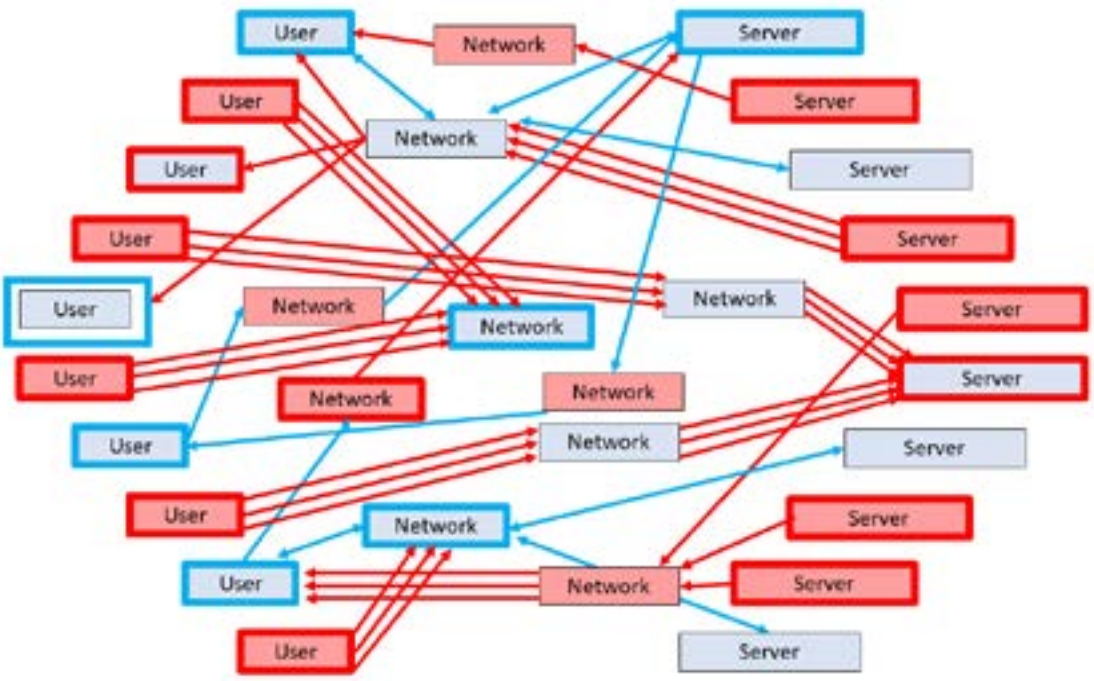
2. Set up the model by distributing the following items:

- nametags to indicate students' roles as Users, Network Devices, or Servers
- blue and red objects indicating Blue and Red Teams (half the Users, Network Devices, and Servers should be on each team)
- index cards and pencils for students to send requests and responses
- cards cut from *User Information Cards* (English | Spanish Coming Soon)

3. Give both teams time to strategize.

- Give Red Team students copies of *Red Team Suggestions* (English | Spanish Coming Soon).
- Give Blue Team students copies of *Blue Team Suggestions* (English | Spanish Coming Soon) or let them reference the cybersecurity ideas recorded in Part One. You can provide them with envelopes.

4. Run the model again. As necessary, remind students to refrain from physically interfering with each other.



5. After the model has run for several minutes, have every student switch their object and copy of Team Suggestions with a member of the other Team. Give both teams a few minutes to strategize. Then run the model again.

Activity Tips

As time and interest permit, you can also have students change roles among Users, Network Devices, and Servers.

6. Pause the model. Ask:

> **Q: What were some of the things the Blue Team did?**
>
> *A: Accept all responses. Possible responses include refusing to accept or reply to suspicious responses, checking for viruses, concealing requests so they couldn't be read by Network Devices, and refusing to accept large numbers of messages.*

Record students' answers on a whiteboard, chart paper, or some other medium for later reference.

7. If you plan to teach the Encryption Extension, ask:

> **Q: How did the Blue Team prevent eavesdropping?**
>
> *A: Responses will vary. Possible responses include folding up index cards, putting them in envelopes, or using some other method to make them difficult to read.*

Remind students that these techniques are models of encryption, changing data into a form that unauthorized parties cannot understand.

8. Connect the model to the real world by asking:

> **Q: Have you used any of the cybersecurity techniques in this model in real life? Which ones?**
>
> *A: Responses will vary. Possible responses include not opening or responding to suspicious messages and installing antivirus software.*

> **Q: Can you think of any cybersecurity techniques that weren't included in our model? What are they?**
>
> *A: Responses will vary. Possible responses include using strong passwords and having lock mechanisms, such as face, eye, or thumb scans.*

Vocabulary Tips

If students bring up the idea of passwords or lock mechanisms, tell them that authentication is the cybersecurity term for the verification of a person's identity. Authentication can take the form of passwords, challenge questions, body scans, or the presence of other devices or accounts (multi-factor authentication).

Give every student a copy of *Cybersecurity Reference* (English | Spanish Coming Soon) to take home for future reference. Explain that they can help their families and other people they care about by sharing their knowledge of cybersecurity.

9. Explain that, in addition to protecting just themselves and the people around them, students can protect lots of people by pursuing careers in cybersecurity. To illustrate some of these careers, play the video *Cybersecurity: Working with Puzzles* (3:40).

watch video

Ask

> **Q: Why is it helpful for people to have careers in cybersecurity?**
>
> *A: Responses will vary. A possible response: cybersecurity professionals protect people's data so they can safely use the Internet for communicating, learning, and having fun. They find security weaknesses so they can be fixed before they are used for bad purposes.*

Students may believe they need to know lots of math or coding to have a cybersecurity job. Emphasize that many cybersecurity professionals do not need to know advanced math or coding. They mostly need to be curious about how things work, how they can be broken, and how to protect them. Encourage students to use cybersecurity practices in their own lives and learn more about cybersecurity careers.

10. Wrap up the lessons by revisiting the questions from the beginning of Lesson 1 and allowing students to refine their answers:

> **Q: What is the Internet?**
>
> *A: Responses will vary. A possible response: the Internet is a network of computer networks around the world. It allows users to submit requests via computers. Network devices transmit these requests to servers, which process them and provide responses. Network devices carry the responses back to the users who made the requests.*

> **Q: How can we be safe when using the Internet?**
>
> *A: Responses will vary. A possible response: we can use cybersecurity, which is the protection of computers, data, and identity. It is conducted by ordinary individuals and professionals. Cybersecurity professionals use the mindsets of a defensive Blue Team and an offensive Red Team to make security as effective as possible. Cybersecurity techniques include security awareness, antivirus software, encryption, and firewalls.*

Extension Activity: Encryption

Use the following activity either during or after the lesson to extend student mastery of this Grades 6–8 standard.

> **2.NI.06.** Apply multiple methods of encryption to model the secure transmission of information.
>
> Encryption can be as simple as letter substitution or as complicated as modern methods used to secure networks and the Internet. Students should encode and decode messages using a variety of encryption methods, and they should understand the different levels of complexity used to hide or secure information.

1. Begin by reviewing what students have learned so far about encryption. Ask:

> **Q: What do you already know about encryption?**
>
> *A: Accept all responses. A possible response is that encryption means using a secret code to change data into a form that others cannot understand.*

> **Q: How did we represent encryption in our model of the Internet?**
>
> *A: Responses will vary. Possible responses include folding up index cards and sealing index cards inside of envelopes to hide it.*

2. Tell students that they are now going to learn some methods of converting data that are closer to the encryption techniques used on the Internet.

3. Put the following message somewhere where all students can read it (such as on a whiteboard, on chart paper, in a shared document):

This sentence is a secret message.

Ask:

> **Q: Besides folding it up or covering it, what could I do to this sentence to make it harder for most people to understand?**
>
> *A: Accept all responses. Possible responses include rearranging the letters or replacing them with other letters, numbers, or symbols.*

4. Explain that methods of converting data into hard-to-understand forms are known as ciphers. Students have just described different kinds of ciphers.

5. Explain that ciphers that rearrange the letters (and other characters) in a message are called transposition ciphers. Students may have described some specific transposition ciphers already, and they may be familiar with others. Ask:

> **Q: Can you think of ways that people rearrange letters in messages? What are they?**
>
> *A: Accept all responses. Possible responses include writing a message backward or using "Pig Latin," a method of word transformation in which the initial consonant or consonant cluster is moved to the end of each word and a vowel sound added afterward. (For example, in Pig Latin, the above message might be "Isthay entencesay isyay ayay ecretsay essagemay." The addition of vowel sounds after each word means Pig Latin is not a pure transposition cipher, but it may be close enough for student understanding.)*

Vocabulary Tips

Explain that the word transposition comes from the Latin roots trans (meaning across) and ponere (meaning to place). Have students think about how uses of the word transposition in other contexts relate to its roots. For example, it has specific meanings in subjects such as algebra, geometry, music, and genetics. All those meanings are related in some way to the idea of an entity being "placed across," or changing its position.

6. Explain that there are many ways to rearrange the characters in a message. Give each student a copy of *Transposition Ciphers* (English | Spanish Coming Soon) so they can encounter some examples. Work through one example as a class. You might use column transposition, in which the message is written downward in columns of a given length and then transcribed from left to right. So the message

This sentence is a secret message.

would be written in 5-character columns as

ECSTA
HNEEMG
ITICEE
SESRS
SNAES

then transcribed from left to right as

Tecsta hneemg iticee sesrs snaes

7. Explain that the original sentence is known as the plaintext, while the hard-to-understand new sentence is known as the ciphertext. When you encrypt something, you convert it from plaintext to ciphertext.

8. Ask:

> **Q: How could we convert this ciphertext back into plaintext?**
>
> *A: Responses will vary. A possible response is by decoding it, or running the encryption method in reverse.*

9. Demonstrate how to reverse the process. For example, take the ciphertext message

   Tecsta hneemg iticee sesrs snaes

   and write it in 6-or-5-character rows as

TECSTA
HNEEMG
ITICEE
SESRS
SNAES

Then transcribe the rows from top to bottom as

This sentence is a secret message.

Explain that when you convert text from ciphertext back to plaintext, you are decrypting it.

10. To practice transposition ciphers,

- have students form pairs.
- have each pair select one transposition cipher from *Transposition Ciphers* (English | Spanish Coming Soon) to use.

- have every student make up a brief sentence and write the plaintext form on an index card and the ciphertext form on a second index card.

- have students swap ciphertexts with their partners and attempt to decrypt each other's ciphertexts.

11. Once students are familiar with transposition ciphers, explain that another important kind of cipher is called a substitution cipher. Students may have described some specific substitution ciphers already, and they may be familiar with others. Ask:

> **Q: Can you think of ways people replace letters in messages with other letters, numbers, or symbols? What are they?**
>
> *A: Accept all responses. Possible responses include replacing each letter of the alphabet with a corresponding number (e.g., A=1, B=2) or using a word processor font that replaces letters with symbols.*

Vocabulary Tips

Explain that the word substitution comes from the Latin roots *sub* (meaning **beneath**) and *stare* (meaning *to stand*). Have students think about how uses of the word *substitution* in other contexts relate to its roots. For example, it has specific meanings in subjects such as algebra, sports, and genetics. All those meanings are related in some way to the idea of one entity "standing beneath," or being replaced by, another.

12. Explain that there are many ways to substitute the characters in a message for others. Give each student a copy of *Substitution Ciphers* (English | Spanish Coming Soon) so they can encounter some examples. Work through one example as a class. You might use a shift cipher, in which each letter is replaced by a different letter a certain distance later in the alphabet. So the message

    This sentence is a secret message.

    if each letter were replaced by a letter three later in the alphabet, as shown

    ```
    Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Ciphertext: DEFGHIJKLMNOPQRSTUVWXYZABC
    ```

    would be written as

    Wklv vhqwhqfh lv d vhfuhw phvvdjh

13. Ask:

> **Q: How could we convert this ciphertext back into plaintext?**
>
> *A: Responses will vary. A possible response is by decrypting, or running the encryption method in reverse.*

14. Demonstrate how the process can be reversed by taking the ciphertext message

    Wklv vhqwhqfh lv d vhfuhw phvvdjh

    And replacing each letter with the one three before it in the alphabet to give

    This sentence is a secret message.

15. To practice substitution ciphers,

- have students form pairs.
- have each pair select one substitution cipher from Substitution Ciphers (English | Spanish) to use.
- have every student make up a brief sentence and write the plaintext form on an index card and the ciphertext form on a second index card.
- have students swap ciphertexts with their partners and attempt to decrypt each other's ciphers.

16. Once students are familiar with transposition and substitution ciphers, you can run the Internet model again and have them use such ciphers in their requests and responses.

17. After running the model with encryption, ask:

> **Q: Did encryption help to prevent cyberattacks? Why or why not?**
>
> *A: Responses will vary. A possible response is that encryption made it harder for the Red Team to eavesdrop on messages in transit.*

> **Q: Did you encounter any problems when using encryption? What were they?**
>
> *A: Responses will vary. Possible responses: Red Team players may have figured out how to decrypt messages. Blue Team players may not have known which ciphers other Blue Team players were using.*

18. If students are interested, explain that the problem of sharing a key—the information needed to encrypt or decrypt a request or response from a friendly computer—happens on the actual Internet as well as in their model. Users do not want to simply send the key they are using for the same reason that Users in your class model would not want to send a request saying "Future requests will be in a shift cipher that uses letters three spaces later in the alphabet"—namely, if the key is eavesdropped, the eavesdropping attacker will know how to decrypt future requests.

    The current solution to this problem involves the fact that certain mathematical operations are easy to do in one direction but hard to do in the other direction. For example, it is easy to multiply the prime numbers 89 and 97 together, but it is hard to determine the factors of their product, 8,633 (and it gets much, much harder when the prime numbers involved are very large). These mathematical operations can be used to create techniques that, unlike the ciphers students have explored, are easy to use for encryption but hard to use for decryption. As a result, senders can encrypt messages that they themselves cannot decrypt but their intended recipients can. This process is known as *public-key encryption.*

    It's not important for students to understand the details of public-key encryption, but they should understand that it is used on the Internet to keep data secure.

Glossary

Antivirus Software
a computer program that checks for suspicious software and remote-control programs and stops them from working

Attacker
a person who uses the Internet to steal, hurt, or cause damage

Authentication
the verification of a person's identity

Computer
a technology that gets input, stores and processes information, and gives output

Cyberattack
a use of the Internet to steal, hurt, or cause damage

Cybersecurity
the protection of computers, data, and identity

Data
information that computers store and process

Encryption
changing data into a form that unauthorized parties cannot understand

Firewall
a technology that lets only certain requests reach a server or other part of a network

Information
facts

Internet
a network of computer networks around the world

Model
a representation of an object, system, or process

Network Device
a computer or other technology that helps connect users' computers to each other and to servers

Personally Identifiable Information
facts that can be used to identify a particular person

Protocol
a set of rules for computers to send and receive information

Request
a message from a computer to a server asking for information

Response
a message from a server back to another computer as an answer to a request

Security Awareness
being careful when using the Internet

Server
a computer with software that processes requests or provides a service to users

Trade-off
a gain in terms of one factor with a simultaneous loss in terms of another factor

User
a person who accesses the Internet