girls4tech

DIGITAL LESSON BUNDLE

Secure the Network

Objectives

Students will

- Brainstorm a concept for a new company and identify the data it would collect
- Apply probability as they investigate the security behind passwords
- Develop a multi-factor verification strategy to protect their new business network

GRADE RANGE

6–8

DURATION

Two 60–75 minute sessions

OVERVIEW

In this STEM-based digital learning bundle, students will learn about the importance of cybersecurity and how networks are evolving to become more secure. Students will brainstorm an idea for a new company and consider the personal data the company may need to collect. Then, through a series of activities, students will investigate the concept of internet security—including an exploration of ciphers, passwords, dual-factor verification, and biometrics. They will ultimately apply what they learned as they use the principals of zero trust architecture to create an online security map for their new business.

BACKGROUND

As hackers become savvier and information is more rapidly shared online, networks that rely on a single password security system leave themselves increasingly vulnerable to data breeches. To ensure that companies' confidential information *remains* confidential, networks must make their internet security more complex. Websites are encouraged to move towards zero trust architecture, which requires every user to prove their identity each time they enter, and even each time different data is accessed. In addition, dual- and/or multi-factor authentication requires website users to prove their identity in two or more ways, such as entering complex passwords, providing personal information, and/or sharing biometrics. This authentication, especially when combined with zero trust architecture, decreases the risk of successful cyberattacks and better protects personal information.

MATERIALS

All Sessions

- Device to project slides (1)

Session 1

- **Create a Company** handout (1 per student pair)
- Capture Sheet (1 per student)

Station: All About Ciphers

- **All About Ciphers** handout (1 per student)

Station: Create a Password

- **Create a Password** handout (1 per student)
- Calculators (5–7)

Station: Two-Factor Verification

- Two-Factor Verification Instructions (10 copies)
- Two-Factor Verification Script (10 copies)
- Two-Factor Verification Personal Information Sheet (1 per student)
- Devices with internet access (5)

Station: Biometrics

- Facial Map Squares (1 per student)
- Class Face Map Grid (1 copy)
- Class Fingerprint Grid (1 copy)
- Ink pad (1–2)
- Scrap paper (10)
- Glue sticks (2)
- Colored pencils
- Small mirrors (3–5)
- Device for recording voice memos (1)*
- **Session 1 Conclusions** handout (1 per student)
- ***Note:** *Before class begins, create a set of instructions detailing how students can record, save, and listen to voice memos on this device.*

Session 2

- Completed **Create a Company** handout from Session 1 (1 per student)
- Completed **Capture Sheets** from Session 1 (1 per student)
- **Security Map** handout (1 per student pair)
- Posterboard or another large piece of paper (1 per student pair)
- Scissors (5)
- Tape or glue sticks (3)
- Drawing materials (for the class to share)

EDUCATOR PREPARATION

- Before each session, make sure to copy and prepare the required handouts and materials.
- Before the first session, prepare the four stations around the classroom.
- If students are learning virtually:
    - They may print out the handouts at home or utilize shared online documents. You can also make them available through your chosen virtual learning platform or learning management system.
    - If an activity calls for working with a partner or group, students learning virtually can share their answers out loud, add to a live/shared document, or comment in a chat box. Alternatively, you can prepare breakout rooms in your learning management system prior to your session.
    - Platforms like Zoom allow you to pre-assign participants to breakout rooms. Google Meet will randomly distribute participants.

USING THIS GUIDE

The goal of this guide is to give educators a complete set of resources for facilitating lessons on internet security. It provides slide-by-slide instructions to ensure educators are prepared to explain, discuss, and facilitate the hands-on content in the presentation. The presentation is designed to cover two class sessions, but it can be flexible depending on the students' needs and the time available. However, the content should be presented in order.

The accompanying presentation was created with PowerPoint so that it can be used in a variety of classrooms. If you are using a laptop with a projector, simply progress through the PowerPoint by clicking to advance. All of the interactive aspects of the presentation are set to occur on click. This includes images, text boxes, and links which will appear in your web browser. If you are using an interactive whiteboard, tap each slide with your finger or stylus to activate the interactive aspects of the presentation. Notes for each slide provide information on how to proceed.

PROCEDURE

Session 1 (Slides 1–5)

Overview

Students will be introduced to the idea of a digital footprint and the importance of keeping website data secure. They will brainstorm an idea for their own company and consider the information it may need to collect from its customers. They will then rotate through stations as they explore concepts related to security.

Slide 1

- Click once and ask students to share answers to: What do you use the internet for?
- Encourage students to turn to a partner and brainstorm as many different ways that they use the internet as they can in one minute.
- Regain the class's attention when one minute is complete.

Slide 2

- Tell the class that every time someone uses the internet, they leave behind a trail of personal data or information.
- Explain that this trail of data is called their digital footprint.
- Click twice and read through the sample list of data that someone can leave behind on the internet.
- Then ask students: Why could it be dangerous to leave this data behind?
- Explain that:
    - Hackers are cybercriminals who try to break into websites and networks and steal personal data. They then give this information to other cybercriminals who can use it in all kinds of ways.
    - While sharing this data can make our lives easier (for instance, we can have packages delivered to our doors!), we also have to make sure that our data is only used by the people who are supposed to have it.

Slide 3

- Divide students into pairs and explain that each pair will now think about the importance of protecting personal data from the perspective of a company.
- Distribute one **Create a Company** handout to each pair and review the directions provided.
- Give students about 10 minutes to collaborate and complete each of the steps.
- Then bring the class back together and discuss students' responses to the handout's third question.

Slide 4

- Reiterate that internet security is important because it keeps personal information safe and protects it from cybercriminals who may try to use it in bad ways.
- Tell the class that they will be working in stations to investigate this idea of internet security for the rest of the class session.

- Preview that the stations will explore the topics of ciphers, passwords, dual-factor verification, and biometrics. Then show students where they can find the four stations located around the classroom.
- Prepare students for their station activities by performing the following:
    - Assign each pair a starting point. Explain that you will be giving timing reminders to keep them on track. Students can rotate clockwise to the next station each time they finish the activity.
    - Pass out one **Capture Sheet** to each student and explain that each square corresponds with one station.
    - Explain that student pairs should carefully read the directions at each station in order to complete the activity. The final step will always be to record information on their **Capture Sheet**.
- Then encourage students to go to their first station and begin!
- Click the timer to begin the countdown. Every 10–15 minutes, encourage students to move on to the next station if they haven't already.
- As students finish all four stations, give them a **Session 1: Conclusions** handout (one half-sheet per student). They may work on this until there are about 5 minutes left in the class session and/or the rest of the class is also done with their station work.

Slide 5

- When there are at least five minutes left in the class session, regroup as a class.
- Click to display the question presented on the **Session 1: Conclusions** handout and read it aloud.
- Based on the time left in the session, either discuss this question as a class *or* assign students to jot their ideas on the handout for homework.

Session 2 (Slides 6–13)

Overview

After learning about the concept of zero trust architecture, students will create an online security map for their new business's website. They will apply what they have learned over the two sessions as they consider how both customers and employees could access and use the website in a secure environment.

Slide 6

- Bring students' attention to the castle image on the slide.
- Ask them to imagine that the castle represents the business they brainstormed last session. Inside the castle rests all the personal information that their business has collected from customers.
- Click once to add a moat, bridge, and guard to the image.
- Encourage students to pretend that this entry point represents how someone logs in into their business's website.
- Then ask: Would you say that this entryway represents a safe and secure login or an unsafe login? Why?
- Help students understand that this image represents an unsafe login. Any website with only one guard and entry point (such as a password) is not as safe and secure as it could be.
- Ask students to think/pair/share: How could this castle be made safer and more secure against intruders?

Slide 7

- Tell the class that a more secure way to access a website and navigate within it is called zero trust architecture. Explain that architecture is the design of how something is built.
- Click and explain that in zero trust architecture, no one is trusted at the entry point—even if the guard recognizes you! There is always a security check.
- Then click to show the image of the castle, this time with guards in many different areas.
- Explain that with zero trust architecture, all important pieces of information are protected separately. Even once someone is inside, they must pass through a security checkpoint every time they want to access a new piece of important information.

Slides 8

- Ask: What may be the advantages and disadvantages of zero trust architecture?
- Encourage students to help you fill out the T-Chart.
- Be sure students understand that:
    - Disadvantages may include that it takes longer to log in and/or for people who work at the company to access information.
    - Advantages include that it is harder for someone to break into the website *and* if the website is hacked, all of the data is not immediately at risk!

Slide 9

- In addition to having multiple security checkpoints, explain that these checkpoints could also use dual or multi-factor verification.
- Ask: Based on what you learned about dual-factor verification, what do you think multi-factor verification is?
- Click and explain that multi-factor verification is one step up from dual-factor verification. In multi-factor verification, the user's identity is verified using three main categories: something you know, something you have, and something you are.
- Ask for student ideas about what each category may include before you click to show and read the examples.
- Tell students that just as dual-factor verification is stronger than a system that uses a single step for logging in, adding this third step can make the log-in even more secure and harder to crack!

Slide 10

- Tell students that for the rest of the class session, they will be challenged to apply what they have learned as they think through the security of their new company's website.
- Click and ask: Who are the two main groups who will have to access your website?
- Click again and help students understand that there are two different entry points that will need to be protected:
    - How the **customer** logs in, gives their personal information, and purchases an item or service
    - How **someone who works at your company** logs in and accesses the customers' information

Slide 11

- Prepare students for the activity by performing the following:
    - Ask students to take out their completed **Create a Company** and **Capture Sheet** handouts from Session 1.
    - Distribute one **Security Map** handout to each pair and review the steps together.
    - Remind students that their goal is to create a website that is as secure as possible. Encourage them to think about the topics they have learned about, as well as the information recorded on their **Create a Company** and **Capture Sheet** handouts.
    - *Optional:* For students who may need additional guidance, click twice to display a sample security map, and review it together. Explain that pairs may use this map as a model as they create their own.
    - Distribute one posterboard or large piece of paper to each pair, and show students where they can find the scissors, glue, and coloring supplies.
- Then encourage pairs to begin!

Slide 12

- When there are 10–15 minutes left in the class session, encourage pairs to share their maps with another group and explain the security measures that a customer and a member of the company would face.
- Challenge each pair to suggest one additional way that their peers could strengthen their security map.

Slide 13

- Conclude with a full-class discussion around the question presented on the slide: How can you apply the concepts you have learned over these two class sessions to help your personal data stay safe online?

CONTENT AREA STANDARDS

Next Generation Science Standards (NGSS)—Crosscutting Concepts

- MS-ETS1-1. The uses of technologies and limitations on their uses are driven by individual or societal needs, desires, and values.

Technology Standards for Technological and Engineering Literacy

- Standard 4: The Cultural, Social, Economic, and Political Effects of Technology
  In order to recognize the changes in society caused by the use of technology, students should learn that:
    - E. Technology, by itself, is neither good nor bad, but decisions about the use of products and systems can result in desirable or undesirable consequences.
- Standard 8: The Attributes of Design: In order to realize the attributes of design, students should learn that:
    - G. Requirements for design are made up of criteria and constraints.

Common Core Mathematics Standards

- CCSS.MATH.CONTENT.6.SP.B.5: Summarize numerical data sets in relation to their context, such as by:
    - CCSS.MATH.CONTENT.6.SP.B.5.A: Reporting the number of observations.
- CCSS.MATH.CONTENT.7.SP.C.8: Find probabilities of compound events using organized lists, tables, tree diagrams, and simulation.

ELA Common Core State Standards (CCSS)

- CCSS.ELA-LITERACY.CCRA.SL.1: Prepare for and participate effectively in a range of conversations and collaborations with diverse partners, building on others' ideas and expressing their own clearly and persuasively.
- CCSS.ELA-LITERACY.CCRA.SL.5: Make strategic use of digital media and visual displays of data to express information and enhance understanding of presentations.

Create a Company

1. **Brainstorm**—With a partner, brainstorm ideas for a new company. The company must sell goods (physical products) or services (things that people do). Record your ideas below, and then circle your favorite idea.

2. **Consider**—If your company creates a website to sell its goods or services to customers online, what online data (or information) would it need from customers in order to be successful?

3. **Discuss**—If your company used the internet to collect all of the data above, why must you make sure the data stays secure and only in the hands of your company?

Create a Company

All About Ciphers	Create a Password!
+ **-**	Tips – 1. 2. 3.
Two-Factor Verification	**Biometrics**
Pros: Cons:	_____ _____ _____ _____ _____ _____ _____

All About Ciphers

Carefully read and complete each section with your partner as you learn about ciphers.

Part 1: Read & Learn

A cipher is a system designed to secretly transmit information by changing or rearranging the message's letters.

When you encipher a message, you convert the information from regular words into a secret message written in "cipher text."

When you decipher a message, you convert a secret message in cipher text back into regular words. In order to encipher or decipher a message, you need a key that explains how to transform the message.

One of the most popular ciphers is called the Caesar Cipher. In a Caesar Cipher, the key tells you how many times the letters in the alphabet are shifted. For instance:

If the key is +2, then A becomes C, B becomes D...all the way to Z becomes B, as shown in the chart below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z																								

If the key is +6, then A becomes G, B becomes H...all the way until Z becomes F, as shown in the chart below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

						A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z																				

Part 2: Encipher & Decipher

Step 1: Secretly record a message you would like to encipher here. Your partner should not see your message! Try to write between two and five words.

Message: _____

Step 2: Select a key. Your key needs to have a plus or minus, as well as a number of shifts. Once you've written your key, fill in the alphabet chart below to help you encipher your message.

Key: _____

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Step 4: Encipher your message on a piece of scrap paper so it can be transmitted safely.

Step 5: Exchange encrypted messages with your partner. Give each other a moment to try to decipher each other's messages without the key. Can you figure it out? Then share your keys with each other and decipher each other's messages.

Part 3: Discuss & Jot

In the All About Ciphers square of your Capture Sheet, record:

+ How could ciphers make transmitting information more secure?

- Could risks still exist when using ciphers to transmit information? Why or why not?

Create a Password!

Carefully read and complete each section with your partner as you learn about passwords.

Part 1: Read & Learn

Did you know that passwords are examples of permutations? A permutation is a way of arranging a group of things in a certain order. ABCD, for example, is one permutation of four letters, and DBCA is another permutation of four letters.

In this station, you will investigate different password permutations and the probability (or chance) of someone else guessing your password.

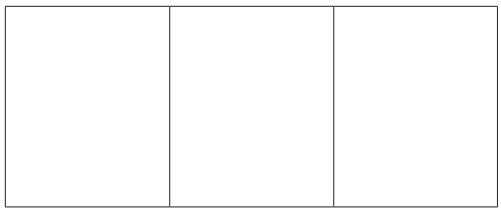
Part 2: Explore

Challenge 1

1. Use the numbers 1, 2, and/or 3 to create a secret 3-digit password. You may use numbers more than once. Do not show your partner!

   Record it here: ____ _____ ____

2. Test the probability: Ask your partner to guess your password, one digit at a time. When they guess the correct number, tell them to move on to the next digit. Keep track of their guesses below:



   Total guesses: _____ _____ _____

3. Work with your partner to **calculate** the probability. What are the chances of someone guessing the password the **first time** if they knew you only used the numbers 1–3?

   Fill in the blanks to figure it out:

   There is a 1 out of ___ chance they would guess the first digit on their first try.

   There is a 1 out of ___ chance they would guess the second digit on their first try.

   There is a 1 out of ___ chance they would guess the third digit on their first try.

   Then multiply these three chances together to calculate the probability of someone guessing the entire password correctly on their first try! Solve it, then check your answer.

$$\frac{1 \times 1 \times 1}{\_\_\_ \times \_\_\_ \times \_\_\_} = \frac{1}{\_\_\_}$$

Answer: 1/27

Challenge 2

Thankfully, there are more than three numbers that can be used when you create a password. There are 10 different numbers, 26 lowercase letters, and 26 uppercase letters...in addition to many different symbols!

Work with your partner as you apply what you learned from the first challenge to calculate the answers below:

- If a password could be any lowercase letter, what is the chance that someone would guess the first letter correctly?

  Answer: 1/26

- If the password could be any lowercase or any uppercase letter, what is the chance that someone would guess the first letter correctly?

  Answer: 1/52

- If the password could be any lowercase or uppercase letter, or 0–9, what is the chance the someone would guess the first letter correctly?

  Answer: 1/61

- If the password consisted of three digits (lowercase or uppercase letter, and/or 0–9), what are the chances that someone would guess the entire password correctly?

  Answer: $\frac{1 \times 1 \times 1}{61 \times 61 \times 61} = \frac{1}{226{,}981}$

- If the password consisted of six digits (lowercase or uppercase letter, and/or 0–9), what are the chances that someone would guess the entire password correctly?

  Answer: $\frac{1 \times 1 \times 1 \times 1 \times 1 \times 1}{61 \times 61 \times 61 \times 61 \times 61 \times 61} = \frac{1}{844{,}596{,}301}$

Discuss & Jot

In the Create a Password! square of your **Capture Sheet**, record:
What tips would you give to someone to make their password as strong as possible?

1.
2.
3.

Two-Factor Verification

Carefully read and complete each section below as you explore two-factor verification.

Part 1: Read & Learn

Two-factor verification means you need two factors—or two things—to prove who you are before you can access your account. It's like having two different locks on something! The extra step helps make sure that the person logging into your account is *really* you.

Part 2: Act Out

1. First, fill out the Personal Information Sheets individually. Then exchange Personal Information Sheets with your partner.
2. You will now act out what two-factor verification looks like when you try to log into a website! Decide which partner will pretend to be the **Website** and which partner will pretend to be the **Internet User**.
3. The **Website** should then follow the instructions on the Script and read it aloud to the **Internet User**. The **Internet User** should follow the commands of the **Website** as they try to log in to their website account.

Part 3: Discuss & Jot

In the Two-Factor Verification square of your **Capture Sheet**, record:

- What are the pros (or advantages) of two-factor verification?
- What are the cons (or disadvantages) of two-factor verification?

If time remains, swap roles and read the script again.

Two-Factor Verification Personal Information Sheet

Instructions: If you create a website account with an adult, the following information may be collected. Pretend that you are creating an online account as you fill out the information below.

---

1. First, create a strong password, using the following guidelines:
    - Make it at least 12 characters long. The longer, the better!
    - Use uppercase letters, lowercase letters, numbers, and symbols.
    - Do not include any personal information.
    - Make sure it is different from any other password you have.

Password: _____

2. Provide information that can be used to confirm your identity if you forget your password:
    - What is your favorite color? _____
    - What is your math teacher's name? _____
    - What town/city were you born in? _____

3. Provide the following personal information:
    - Birthday: _____
    - Zip Code: _____
    - Email Address: _____

Two Factor Verification Script

Instructions: The **Website** should read the script below to the **Internet User**. The **Website** should say the words in italics and read/do the words in bold.

Authentication #1

Thank you for trying to access your account on www.[insert website name].com. For access to this important website, please tell me your password. Be sure to tell me which letters are capitalized.

If the Internet User says their password correctly, move down to Authentication #2.

If the Internet User says their password incorrectly, say: *You have two more times to try giving me your password.*

If they say their password correctly the second or third time, move down to Authentication #2.

If they don't know their password after three tries, ask them one of the following questions:

- *What is your favorite color?*
- *What is your math teacher's name?*
- *What town or city were you born in?*

If they get this answer wrong, say: *You are locked out of your account. Please return in 24 hours and try again.* **[Script is complete!]**

If they get this answer right, say: You must now create a new strong password. Write it down, remember it, and then give it to me.

Once you have their new password, start back at the beginning of the script.

Authentication #2

Now that your password is correct, we still need to confirm your identity.

Choose and move onto one of the following options:

- Option 1:
  - **Use a device to send a made-up code (at least 6 characters) from your email address to your partner's email address.**
  - **Then say:** *Please check your email and tell me the code you received.*
  - **If the code is correct, say:** *We have confirmed your identity. You now have access to this important website.* **[Script is complete!]**
  - **If the code is incorrect, say:** *You have one more try to confirm your identity. Please tell me the code you received.*

- **If the code is correct the second time, say:** *We have confirmed your identity. You now have access to this important website.* **[Script is complete!]**
- **If the code is incorrect the second time, say:** *We're sorry. We have not been able to confirm your identity. You will not be able to access this important website.* **[Script is complete!]**

- Option 2:
  - **Ask your partner for their birthday, zip code, or email address.**
  - **If it is correct, say:** *We have confirmed your identity. You now have access to this important website.* **[Script is complete!]**
  - **If it is incorrect, say:** *You have one more try to confirm your identity. Please try again.*
  - **If they say it correctly the second time, say:** *We have confirmed your identity. You now have access to this important website.* **[Script is complete!]**
  - **If they say it incorrectly the second time, say:** *We're sorry. We have not been able to confirm your identity. You will not be able to access this important website.* **[Script is complete!]**

Biometrics

Carefully read and complete each section below as you learn about biometrics.

Part 1: Read & Learn

Have you heard the term *biometrics* before? The prefix *bio* means "life" and the suffix *metric* means "of or relating to a measurement." When you put these two word-parts together, biometrics is the measurement and analysis of the living traits that make you *you*. Biometrics is a field that uses these unique physical characteristics to confirm people's identities.

For instance: Have you ever seen someone use their face to unlock their phone? This facial recognition is an example of biometrics! A computer system that specializes in facial recognition can create a map of someone's face from a photo or video. This information is then stored in a database among maps of other faces. Each time a face is scanned, it looks through every face map in order to find a match.

Part 2: Explore

1. Discuss with your partner: What are some biometrics that make you unique?
2. Follow the steps below to explore how your facial features, fingerprints, and voice can set you apart from your peers.
    - Facial Features:
        - First, draw a detailed picture of your face on one of the Facial Map squares. Use the mirror to help you include features that make you unique—such as the color of your eyes, the shape of your eyebrows, or any birthmarks or freckles you may have.
        - Then glue your square onto the Class Face Map grid.
    - Fingerprints:
        - Use the ink pad and a piece of scrap paper to practice taking your own fingerprint.
        - Then place a fingerprint of your pointer finger on the Class Fingerprint Grid.
    - Voice Memo:
        - Follow the instructions provided to create and save a voice memo saying, "My name is [insert your name here]."
3. Then observe, compare, and contrast the different facial maps, fingerprints, and voice memos. Discuss with your partner:
    - Can you see how/why these biometrics can be used to confirm your identity?
    - Do we have any other unique biometrics that could be used to confirm our identities?
    - What may be the benefits (or advantages) of using biometrics for internet security?
    - What may be the risks (or disadvantages) of using biometrics for internet security?

Part 3: Discuss & Jot

In the Biometrics square of your **Capture Sheet**, answer the question: What are biometrics and how can they be used to confirm your identity online?

Class Face Map Grid

Directions: Glue your Facial Map into one of the squares below.

Facial Map Squares

Educator Instructions: Cut out these squares in advance and place them at the Biometrics station.

Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square
Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square
Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square
Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square
Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square
Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square	Facial Map Square

Class Fingerprint Grid

Directions: Carefully place your fingerprint into a square below.

Session 1: Conclusions

Many websites are still protected by only a username and password. Based on what you have learned, how could these websites strengthen their security?

Session 1: Conclusions

Many websites are still protected by only a username and password. Based on what you have learned, how could these websites strengthen their security?

Security Map

Instructions: Follow the instructions below as you think through the security of your company's website!

Step 1: On a posterboard or large piece of paper, create a security map for your new company's website.

Your security map must include:

- How your CUSTOMER will use the website:
    - Steps to log in
    - Steps to make a purchase
- How people who work for your COMPANY will use the website:
    - Steps to log in
    - Steps to access the personal information that the customer provided
- oExamples of:
    - Multi-factor verification
    - Zero Trust Architecture

Be creative. How you create and illustrate this information is up to you!

Step 2: In the space below, explain your website security to your customers. How and why does it keep their personal information secure? Record your answer below, and then cut it out and attach it to your map.