Journal of Technology-Integrated Lessons and Teaching
(2022) Volume 1, Issue 2

Cybersecurity: Introduction to Steganography

Aishat Olere Balogun, Indiana University Bloomington

Overview

This is part of a series of lessons that teach 9th-12th graders about cybersecurity. This lesson begins with a reminder to the students about ethics and cybersecurity and is followed by a problem scenario that introduces the topic of steganography. Students are expected to contribute and explore options and solutions to the problem scenario, followed by a lesson on steganography where students will practice creating their own steganography models as examples. This lesson concludes by having the learners exchange their finished projects (a game) for others to decode as they play the game.

Topics: Cybersecurity, Steganography, Malware, Cryptography

Time: 30 to 40 minutes. Multiple class sessions may be required to complete all aspects of the lesson.

Materials

- Computer with internet and Google Drive access
- Cell phones with WIFI and picture taking capacity
- Notepad++ on computers
- Steganography PowerPoint presentation
- Duck1 and Duck2 images with hidden messages
- edureka!, (2019) YouTube video: Steganography Tutorial | How to Hide Text Inside the Image | Cybersecurity Training | Edureka
- SentinelOne (2019) article: Hiding code inside images: How malware uses steganography
- Cameron (n.d.) article With cryptography easier to detect, cybercriminals now hide malware in plain sight. Call It steganography. Here's how it works
- Code of ethics website (Mile2, n.d.)
- Cybersecurity ethics: Establishing a code for your SOC (Van Impe, 2021).
- Cybersecurity in Education: What Teachers, Parents and Students Should Know (Berkeley Boot Camps, n.d.).

Context-at-a-glance

Setting
9th-12th grade female students in a suburban, public high school.

Modality
Face-to-face and hybrid

Class Structure
One of the lessons in an ungraded, student-selected, extracurricular activity (ECA) class that meets for 45 minutes weekly throughout the school year.

Organizational Norms
One of the STEM focused ECA options offered yearlong by the school. Students who participate are STEM focused and exploring various areas of interest. Most students are familiar with the inquiry process.

Learner Characteristics
15 – 25 students signed up to be part of the class which is also a female focused STEM club. Only female students from mixed grades are represented.

Instructor Characteristics
A high school science teacher affiliated with the local university who is interested in cybersecurity taught this class. Guest speakers were routinely invited to participate when the lesson calls for it.

Development Rationale
This lesson was a part of a series of lessons that covered real life implication of cybersecurity starting from ethics through application.

Design Framework
Merrill's Principle of Instructional Design

DOI: 10.13001/jtilt.v1i2.7079

Setup

Make sure the computers/laptops the students will be using have the Notepad++ application installed on it before the start of the lesson. Students will work in small groups to create the project. Students should have the opportunity to explore around the room so they can take pictures to use for the project. A shared Google Drive folder should be opened for the class to submit their finished work and access lesson materials.

Standards

Indiana K-12 Computer Science-Impact and Culture 3-5.IC.2 "Identify the impact of technology (e.g., social networking, cyber bullying, mobile computing and communication, web technologies, cyber security, and virtualization) on personal life and society" (Indiana Department of Education, n.d., p. 10).

Context and Setting

This lesson was developed as a part of a 15-week-long, 45-minute, weekly class about cybersecurity for 9th-12th grade female students in a suburban public high school in midwestern United States. The school is one of the three high schools located in a university town where the student population includes those from multiple countries. Students who signed up to be part of the ECA group/club at the beginning of the school year were subsequently signed up weekly for the allocated time during the particular school day. This provided the opportunity to interact and participate as a group during the school day without fear of missing the school bus home. Students had the option to sign themselves up for the class meeting or the teacher signed them up on the school meeting management system.

This class was taught by a high school science teacher with an interest in technology and cybersecurity who is also affiliated with the local university. As a teacher in the school, she had access to the school wide system, which, made it easier to sign up students, take attendance, and actively encourage students who fit the profile to become part of the group. Typical class size was 15-25 students depending on the workload of the students. Students had the opportunity to opt out of a class meeting if they had work to make up in a required class because those classes took precedent over an ECA class. They could always catch up on the Canvas learning management system because all the materials were available on Canvas. Guest speakers were routinely invited to speak with the students which created opportunities to discuss job opportunities in STEM and how certain aspects of cybersecurity did not require knowledge of programming or coding.

This course was designed to introduce cybersecurity to STEM-focused female students, who are interested in exploring various aspects of STEM, to learn more or in some cases to consider as a future career option. The course was designed to be delivered synchronously and asynchronously using the Canvas learning management system and Google Drive for sharing materials. For asynchronous delivery, due dates can be extended, and articles and videos watched ahead of time before completion of the project. Options can also be given for students to work alone or with a teammate if their schedules align with each other. A discussion and collaborative tool like Google Jamboard or a chat or discussion option on Canvas may be used for asynchronous collaborative work.

The lessons in this cybersecurity series use the discussion format with a real-life scenario starting the discussion. Questions are then provided to prompt the students to contribute what they think based on prior knowledge or experience. Students then interact with the content and practice and create models based on their understanding of what they just learned using the various technological tools available.

The purpose of this lesson is to make the students more knowledgeable about cybersecurity concepts like steganography, especially in the context of cybersecurity risks. During this lesson, italic text identifies questions or prompts for the learners.

Learning Representation

Attention Grabber (3 min)

Access the Introduction to Cybersecurity and Steganography PowerPoint. Show slide 2 on the presentation and read aloud the problem:

DOI: 10.13001/jtilt.v1i2.7079

A group of students were reported for cheating on a test but after investigation there was no proof of how the students got the test questions or answers. The teacher knew they cheated because they all used the same terms for the answers, but they were not seated next to each other in the exam hall. Also, they all missed the four questions which were a last-minute addition to the test by the teacher.

After reviewing the devices and social media presence of the students no shared document was found except some picture memes the students shared as a joke between themselves.

- *How did they cheat?*
- *What do you think happened?*

Give students the opportunity to come up with suggestions and correct any misconceptions. Take note of issues raised that could be addressed later.

Essential Questions

Present the goals and objectives and essential questions of the lessons (Slide 3):

- *What is Steganography?*
- *How can it be used?*
- *How is steganography different from cryptography?*
- *What are the different types of steganography?*

Activate Existing Knowledge

Remind the students about the basics of ethics in the classroom and what they are learning should never be used outside of the classroom or in an actual scenario. Also remind them that it could be a crime to apply what they are learning outside the controlled environment of the classroom. Include the following warning: *do not try this! You will be caught.*

Knowledge Demonstration (10 min)

Introduction to Steganography: Use the edureka! (2019) YouTube video explaining steganography. Play the video starting from 1minute 15 seconds to 3 minutes 40 seconds: Steganography Tutorial | How to Hide Text Inside the Image | Cybersecurity Training | Edureka (1:15 – 3:40).

Discuss the video with the students and answer any questions they have. Refer to the problem question and ask the students the following questions again:

- *How did they cheat?*
- *What do you think happened?*

Listen to their responses and review any altered perceptions. Use the Steganography PowerPoint to discuss steganography and contrast it with cryptography (Slide 6):

Steganography is a technique that can hide code in plain sight, such as within an image file and Cryptography is the practice of writing coded or encrypted messages (SentinelOne, 2019).

Remind students to finish watching the video on their own before the next class. Prompt them to list other ways they think steganography can be used. The following discussion prompts may be used:

- *Describe steganography in your own words?*
- *Mention some positive and negative applications of steganography.*
- *Did you know about steganography before? If yes from where?*

Knowledge Application (10 min)

Have students open a desktop folder to save all downloaded images for the class. Walk them through the technology for this activity (Google Drive, Notepad++, and their cell phones). Tell them to follow the instructions to practice steganography.

Image Download: Share the Steganography PowerPoint with students and instruct them to download the duck1 image from the JTILT website (Slide 7; Figure 1).

Figure 1: Duck image (Bicanski, n.d.).

DOI: 10.13001/jtilt.v1i2.7079

View Image

Class Practice: Follow the instruction to view the image codes (Slide 8):

- *Right click on the image. Select the Open with.*
- *Select Notepad++.*

This will display the bits that make up the image as a set of characters shown on Slide 9 of the presentation (see Figure 2).

Say while Displaying Figure 2: *The Duck picture opened in Notepad++ as a set of character codes. In Steganography, messages can be hidden between the characters* (Slide 9).

Use the following resources to show the various ways information can be hidden using steganography and how steganography can be used for nefarious acts (Slides 10 and 11):

Have a discussion with the students sharing various ways information can be hidden using steganography. Ways this could happen include:

- Using network media to gain access by hiding another code within the downloaded media (Kadhim et al., 2019).
- Embeded components in downloads or shared images which may automatically trigger infection or invasive permissions without the user aware of the dangers (Cameron, n.d.)

It is also advisable to search for recent news reports about steganography to show real life examples.

Download and View Coded Image

Tell the students to download the duck2 image using the same steps and instructions to view the image codes (presented previously).

Give the students a hint on what to look for within the characters (hint: the word *code*). Slide 5 (see Figure 2) shows the image characters after the addition of the secret message (code: *happy go eat at Wendy's*).

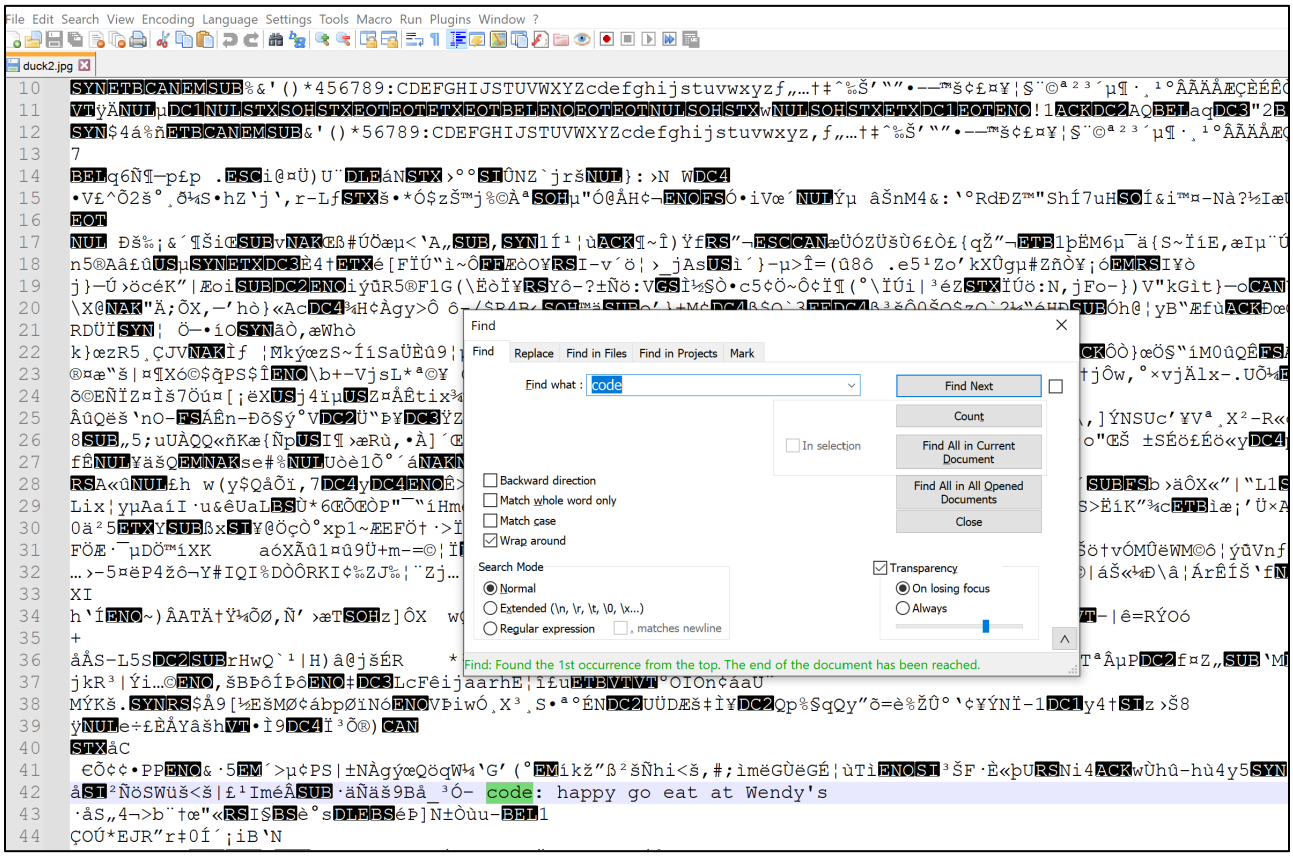

Figure 2: Notepad++ view of the image displaying the message.

DOI: 10.13001/jtilt.v1i2.7079

Practice Project (10 min)

Allow the students to work together in small groups (groups of 4 are ideal) while they complete this project using the following instructions (Slide 14):

Practice: Send your own message:

- *Use your cellphones to take eight original pictures.*
- *Download the pictures to a folder allotted to your team on the shared Google folder. The link will be shared with you.*
- *Create a game using steganography to amend the pictures you took to provide clues.*
- *Share the pictures with the clues on the Google drive.*

Play the Game:

- *Each team will be given the folder of pictures from another group.*
- *The teams should review the pictures using what they have learned about in Stenography to play the game.*
- *Think about how the game could be improved as you play.*

Conclusion (6 min)

Discuss the project with the students and encourage them to share their thoughts about what they learned. Read the first paragraph from the SentinelOne (2019) article referring to the Facebook issue, discuss it with the students to round up the lesson: Hiding code inside images: How malware uses steganography. The following prompts could be used to guide the discussion:

- *Did you know about the Facebook incident mentioned?*
- *Have you learned about other incidences like this?*
- *What advice will you give others based on what you learned from this article?*

Critical Reflection

The lesson was implemented twice but it has been adjusted to include more articles to reflect recent information. The students enjoyed learning about something applicable and it was fun trying to hide information from each other.

Some of the challenges involved students typing the messages in between codes, which will affect the image itself. It is ideal to emphasize that the messages should be included where they see space or at the end of a code line.

Make sure the students create a desktop folder to save items and select the folder as the storage space for downloaded items. Some students always seem to forget the folder name and save the item elsewhere and then they cannot find it. Remember to always reiterate that what they are learning is never to be practiced outside the classroom. It is recommended to provide students a code of ethics form which would be signed by them and a parent or guardian. The form can be edited based on what the instructor and school will allow. The following sites provide examples of what can be on a code of ethics form for a cybersecurity class:

- Code of ethics (Mile2, n.d.).
- Cybersecurity ethics: Establishing a code for your SOC (Van Impe, 2021).

Some changes that would be made to this lesson before the next class is the addition of some type of assessment to determine what the students learned. This is where the use of an exit ticket is recommended with questions like:

- *What new thing did you learn?*
- *What questions do you have?*
- *What did you struggle with?*
- *Explain steganography in your own words*
- *Why do you think you need to know this topic?*

Another addition to this lesson would be to create a collaborative space like a Google Jamboard for students to add questions as the lesson progresses. These questions could be reviewed at the end of class or the start of the next session. This is a great opportunity to address misconceptions or reteach a concept.

A big challenge in this lesson is the struggle to fit the lesson into the recommended time. This can be fixed by completing the lesson in multiple class sessions. It is recommended that the project be explained at the end of the first session while students work on it the next class session. This will give them time to assimilate the information before application.

It is understandable that others might feel conflicted to teach something that could be used for nefarious

DOI: 10.13001/jtilt.v1i2.7079

purposes, but the school environment is an ideal place to guide young students to learn about the ethical use of information. Cybersecurity is something students should be aware of not just as a growing sector for jobs but also to protect themselves.

People are told not to download strange files because it might contain virus or bugs that might affect how the device works or steal personal information. A steganography lesson is an ideal way to teach the students how certain hidden bugs or messages can be created or detected. Instructors are encouraged to emphasize the importance of ethics in cybersecurity at every point of this lesson.

Also, since this is part of a lesson series, instructors can use the information in the Berkeley Boot Camps (n.d.) article to reinforce the importance of cybersecurity: Cybersecurity in education: What teachers, parents and students should know.

References

Berkeley Boot Camps (n.d.). *Cybersecurity in education: What teachers, parents and students should know.* Berkeley Extension. Retrieved September 1, 2022, from https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/

Bicanski. (n.d.) *Beach, duck, mallard, natural habitat, shadow, waterfowl, beak, feather, wildlife, bird.* Pixnio. Retrieved September 1, 2022, from https://pixnio.com/media/beach-duck-mallard-natural-habitat-shadow

Cameron, L. (n.d.). With cryptography easier to detect, cybercriminals now hide malware in plain sight. Call it steganography. Here's how it works. *IEEE Computer Society*. Retrieved September 1, 2022, from https://www.computer.org/publications/tech-news/research/how-steganography-works

edureka! (2019, January 17). *Steganography tutorial: How to hide text inside the image | Cybersecurity training | Edureka* [Video]. YouTube. https://www.youtube.com/watch?v=xepNoHgNj0w

Indiana Department of Education. (n.d.). *Indiana K-12 computer science standards*. Retrieved September 1, 2022, from https://www.in.gov/doe/files/ind-k-12-computer-science-standards.pdf

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326. https://doi.org/10.1016/j.neucom.2018.06.075

Mile2. (n.d.). *Code of ethics*. Retrieved September 1, 2022, from https://www.mile2.com/code-of-ethics/

SentinelOne. (2019, July 4). Hiding code inside images: How malware uses steganography. *SentinelOne Blog.* https://www.sentinelone.com/blog/hiding-code-inside-images-malware-steganography/

Van Impe, K. (2021, January 8). Cybersecurity ethics: Establishing a code for your SOC. *SecurityIntelligence*. https://securityintelligence.com/articles/cybersecurity-ethics-establishing-a-code-of-conduct-for-soc/

About the Author

Aishat Olere Balogun likes to create multiple opportunities for students to extend STEM outside the school/classroom curriculum. Her interests include science education; STEM; and the intersection of technology, learning, and its application to education. She is currently a 9th - 12th grade science teacher, an adjunct professor, and a doctoral student in the Indiana University Bloomington instructional technology department in the school of education.

DOI: 10.13001/jtilt.v1i2.7079