Ruth Abeselom

Professor Duvall

CYSE 368

21 February 2025

# Reflection #1: The First 50 Hours

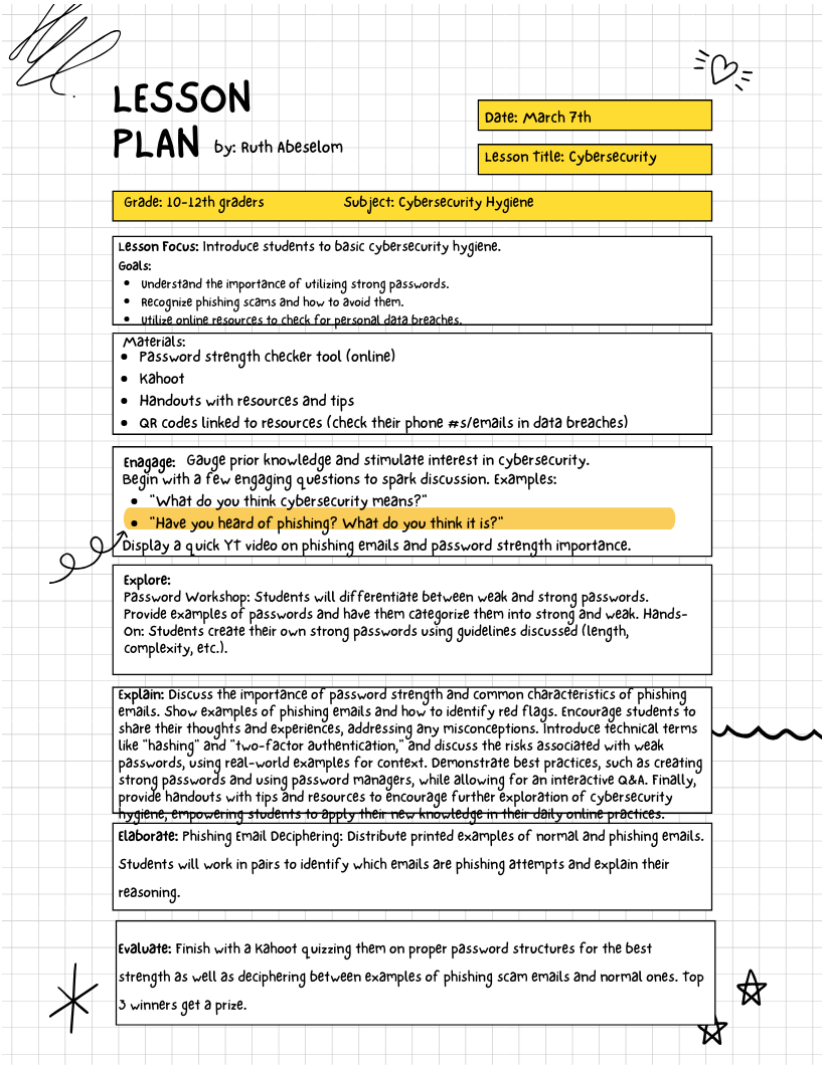
At my orientation training, I was first introduced to the lab staff and given a tour of the lab facilities and the technology encompassing it. The ODU iLab in Newport News contains a lot of cool innovative technology such as 3D printers, laser cutters, a DTG printer, a Cricut maker, a large hydroponic garden system, and much more. I had never used any of this equipment or the technical systems that come with them before other than Tinkercad which is for 3D design, electronics, and coding. All of this new STEM technology that I had to learn and master was somewhat intimidating but I was eased into it all with online and in-person tutorials and demonstrations. I even received a certificate through Canva for learning through their graphic design courses.

Throughout all of this, I was interested in the STEM elements of this experience but wondered when I would encounter the cybersecurity aspects of this internship. After all, cybersecurity students were specifically requested to apply for this experience which is what the other interns and I are all majoring in. This was a concern for some of us as we were mainly planning STEM outreach events for kids and the elderly involving arts and crafts. I am very grateful for the opportunity and experience although the majority of the time is not related to the primary learning objective of attaining technical cybersecurity skills as mentioned.

However, as of this week, we began planning for a Cybersecurity recruitment event that is happening soon at ODU for high school students to get informed and possibly persuade them

to join the Cybersecurity program. We had to formulate ideas for the sessions that are hands-on and engaging while related to major cybersecurity topics. As a result, I would now say a majority of my primary learning objectives are being covered and reached.

In conclusion, my orientation training at the ODU iLab provided an introduction to innovative STEM technologies, despite initial feelings of intimidation. While my focus was primarily on mastering new tools and techniques, I was eager to engage with the cybersecurity aspects of my internship. Although much of my early experience revolved around planning STEM outreach events, the recent opportunity to help organize a Cybersecurity recruitment event has reignited my enthusiasm and aligned my learning objectives with my major. This project will allow me to apply the skills I've learned within the cybersecurity field making this internship a well-rounded and fulfilling experience. Below is my drafted lesson plan for the event pending changes:



LESSON PLAN by: Ruth Abeselom

Date: March 7th

Lesson Title: Cybersecurity

Grade: 10-12th graders Subject: Cybersecurity Hygiene

**Lesson Focus:** Introduce students to basic cybersecurity hygiene.
Goals:
- Understand the importance of utilizing strong passwords.
- Recognize phishing scams and how to avoid them.
- Utilize online resources to check for personal data breaches.

Materials:
- Password strength checker tool (online)
- Kahoot
- Handouts with resources and tips
- QR codes linked to resources (check their phone #s/emails in data breaches)

**Engage:** Gauge prior knowledge and stimulate interest in cybersecurity.
Begin with a few engaging questions to spark discussion. Examples:
- "What do you think cybersecurity means?"
- "Have you heard of phishing? What do you think it is?"

Display a quick YT video on phishing emails and password strength importance.

**Explore:**
Password Workshop: Students will differentiate between weak and strong passwords. Provide examples of passwords and have them categorize them into strong and weak. Hands-On: Students create their own strong passwords using guidelines discussed (length, complexity, etc.).

**Explain:** Discuss the importance of password strength and common characteristics of phishing emails. Show examples of phishing emails and how to identify red flags. Encourage students to share their thoughts and experiences, addressing any misconceptions. Introduce technical terms like "hashing" and "two-factor authentication," and discuss the risks associated with weak passwords, using real-world examples for context. Demonstrate best practices, such as creating strong passwords and using password managers, while allowing for an interactive Q&A. Finally, provide handouts with tips and resources to encourage further exploration of cybersecurity hygiene, empowering students to apply their new knowledge in their daily online practices.

**Elaborate:** Phishing Email Deciphering: Distribute printed examples of normal and phishing emails. Students will work in pairs to identify which emails are phishing attempts and explain their reasoning.

**Evaluate:** Finish with a Kahoot quizzing them on proper password structures for the best strength as well as deciphering between examples of phishing scam emails and normal ones. Top 3 winners get a prize.