

# Cyber Securing the Future

Christopher Kolb,<sup>1, a)</sup> James Strouse,<sup>1, b)</sup> Justynn Palmer,<sup>1, c)</sup> Vitaly Ford,<sup>1, d)</sup> and  
Victoria Turygina<sup>2, e)</sup>

<sup>1)</sup>Arcadia University

450 S Easton Rd, Glenside, PA, USA, 19038

<sup>2)</sup>Ural Federal University

Prospekt Lenina, 51, Yekaterinburg, Sverdlovskaya oblast', Russia, 620075

<sup>a)</sup>Electronic mail: ckolb@arcadia.edu

<sup>b)</sup>Electronic mail: jstrouse@arcadia.edu

<sup>c)</sup>Electronic mail: jpalmer\_01@arcadia.edu

<sup>d)</sup>Corresponding author: fordv@arcadia.edu

<sup>e)</sup>Electronic mail: v.f.volodina@urfu.ru

**Abstract.** Many high school computer science programs do not touch on the field of cybersecurity, meaning a large number of students is not exposed to such important knowledge and career opportunities until at least college. In this project, we aimed at increasing awareness and knowledge of the cybersecurity field in a pre-college environment. We developed multiple lessons using various teaching strategies with the main purpose being to increase knowledge and secondary purpose of determining if students retain knowledge better through a hands-on learning experience or through lectures. In our results, many students expressed that their knowledge in the field of cybersecurity has increased, as well as their interest in it. The pre-lecture survey also stated that many students were not overly familiar with anything besides basic password security before our lessons. While both classes rated their understanding of the field at around the same level, the class that we did the more hands-on experience with rated that the lesson was more interesting and worth the time. These responses, combined with the ever-growing importance of cybersecurity in the modern world, suggests that introducing cybersecurity to general high school level computer science curriculum would be of great benefit to the students.

## INTRODUCTION

Cybersecurity is an ever growing field in today's technology filled society. With the creation of new devices and systems, there is a constant need for professionals to secure them to stop data leaks. Experts predict that by the year 2021 there will be 3.5 million job openings in the field of cybersecurity alone [1]. With the ever growing need for jobs, it is important to increase knowledge of the field as well as introduce opportunities to those who are going through the education system. Our goal for this project was to introduce high school students to cybersecurity basics, careers, and Internet safety. A high school general curriculum has little to no lessons on the basics of cybersecurity and Internet safety. Thus, we sought to increase students' knowledge and understanding of cybersecurity terminology, inform them of career paths within the field, and increase their security on the web, airports, and public networks. While doing this, we also aimed at determining whether the students retain knowledge more when learning cybersecurity topics in a hands-on setting or a hands-off setting.

## BACKGROUND

There has been much research and studies done in identifying the effectiveness of hands-on learning in K-12 education [2, 3, 4]. In Korwin and Jones' study, "*Do Hands-On, Technology-Based Activities Enhance Learning by Reinforcing Cognitive Knowledge and Retention?*" [4], they sought to test hands-on learning retention and engagement against a purely lecture based technological lesson. They taught two classes, class A which they taught with an interactive lesson that got the students more involved, and class B which learned the material through a more traditional lecture. Afterward, they gave both classes the same test and took the mean of the scores based on the total amount of students. Two weeks later, they gave both classes the same test again in order to test their retention. Their results found that there was a significant difference between the immediate knowledge as well as the amount of retention of the material itself. Class A, which received the hands-on lecture had higher means in both of the tests by a statistically significant amount. This shows that hands-on strategies have a higher retention rate of knowledge both long and short term than hands-off learning.

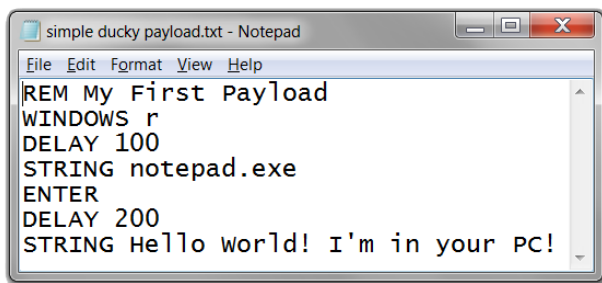
In another study, *PicoCTF: A game-based computer security competition for high school students* [5], Chapman, Burket and Brumley set out to create a program called PicoCTF to create an engaging way to learn about cybersecurity. They hosted a competition for high school students and measured what the students thought about the program. The results demonstrated that this program was able to keep students engaged no matter what their knowledge level was. While this study does not necessarily compare the students' engagement with a hands-off approach, it further reinforces that students react well to hands-on lessons.

## METHODS

Our primary goal in this project was to grant high school students an opportunity to engage in learning about cybersecurity that they often are not able to do until the college level. We focused on creating two lesson plans: one covering the basics of cybersecurity and potential careers in the field, and the other focusing on more in-depth ideas of the cybersecurity field and Internet safety.

We found a local high school that was willing to give us some class time to implement our lessons, and then we created two PowerPoint presentations for each of the provided class periods. We modeled our presentations based on our lesson plans and separated the two classes with class *A* getting the hands-off lesson, and class *B* getting the hands-on. We had both classes participate in identical pre-lesson and post-lesson surveys. The surveys asked the students questions that had them rate their knowledge and comfort level with cybersecurity topics.

We also prepared two devices to show the students some tools that can be used in the field. The two devices that we decided to showcase were a Rubber Ducky Drive [6] and a WiFi Pineapple [7]. A Rubber Ducky Drive is a small device that looks like a normal USB drive. It is one of the hallmark tools of a modern-day hacker and penetration tester. The scripting language used for the device is simple for anyone to understand as shown in Figure 1 and in the wrong hands, it could be catastrophic to a system where it has been deployed.

A screenshot of a Notepad window titled "simple ducky payload.txt - Notepad". The window contains the following text:

```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

**FIGURE 1.** A basic example of Ducky Script.

When plugged into a computer, the Rubber Ducky device is recognized as a keyboard, not as a storage unit. Being recognized as a keyboard, this device opens up unteathered access to the victim's computer. As soon as it is plugged in, it immediately begins to unload its payload onto the computer, pulling up Command Windows searching through confidential files, installing malicious software, reading memory, or dumping user's credentials. Anything that can easily be done with a keyboard – can be done with a Rubber Ducky. The payload can search for files, pull them, and post them at an external public pastebin server in under 30 seconds.

The reason that we chose to go over the Rubber Ducky in our presentation is what was said above: it is hard to recognize it as a threat and easy to use in anyone's hands. We showed the students a simple script that opened up a YouTube video and set the volume to the max, explaining them all of the other applications the Rubber Ducky could have, good and bad. The demonstration of the inherent dangers of inserting random USB devices into their computers provided us with a visual tool carrying a powerful message that was received well throughout the class. We told them how easy it could be for anyone to get a hold of one, while being cautious and not showing them directly where they could buy it.

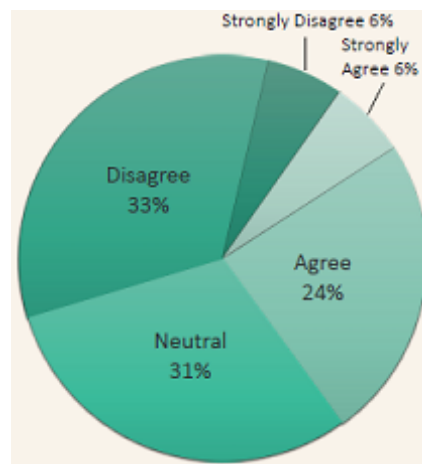
The other device we used to demonstrate the practical applications of different kinds of hacking during the second class was a WiFi Pineapple. There are currently two models available for public use: the WiFi Pineapple NANO and the WiFi Pineapple TETRA. For the purposes of our study, we used the NANO version. The base functionality of both devices is to provide with multipurpose client radios that can function as a Wireless Access Point (WAP), router,

and traffic monitor, all at once. The only significant differences between the aforementioned NANO and TETRA are that the former is compact but can only handle broadcast frequencies up to 2.4 GHz and the latter is double the size but can go up to 5 GHz and has more local memory.

Regarding the lesson in question, we utilized the WiFi Pineapple's WAP and traffic monitoring functionalities via a software interface called "Pine AP" to demonstrate a "man in the middle" attack. That is to say, we used the WiFi Pineapple to impersonate the high school's public wireless access point and then showed the students all of the data that could be collected from anyone unfortunate enough to browse the Internet while connected to it. In order to avoid compromising the security of any students, staff, or faculty, we only used our own personal cell phones to connect to the pineapple and used throwaway credentials to log into an animation forum called [hyunsdojo.com](http://hyunsdojo.com). Despite numerous subsequent queries from the students on how and where to acquire a WiFi Pineapple for themselves, we refused to disclose any concrete information to them. Other than showing them the devices and their functionality, we also showed them resources such as [haveibeenpwned.com](http://haveibeenpwned.com), a website that stores hashes of compromised passwords and allows to securely verify if the password and email address have been previously compromised.

Both the Rubber Ducky and WiFi Pineapple were used in the hands-on and hands-off classes. The hands-on class was given an opportunity and allocated time to interact with the devices and access resources that we provided to them. In the hands-off class, we still showed them the same resources and devices, however, they were not provided time in class to access them. As a result of the time trade-off, we naturally spent more time during the question-answer session in the hands-off class than in the hands-on class.

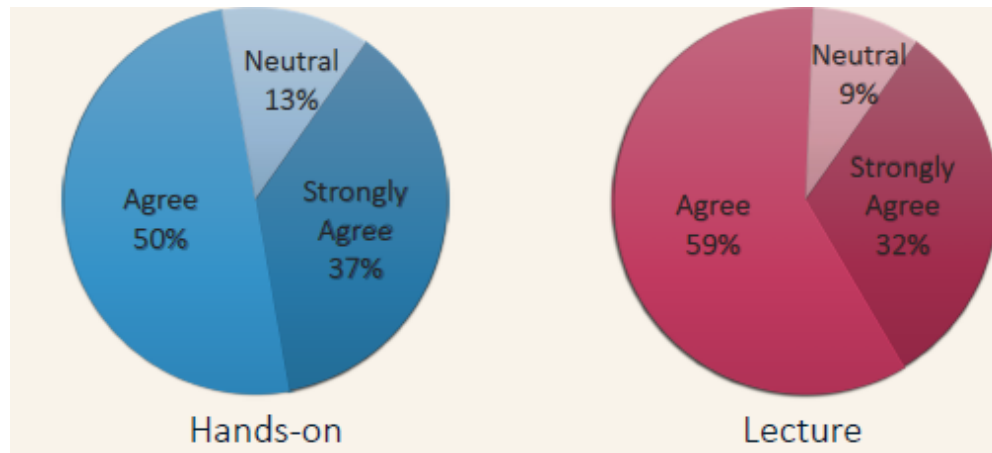
We combined the survey questions to one statement that said "I am comfortable with cybersecurity topics". Looking at the pre-lesson survey in Figure 2, we can acknowledge that most students responded to our pre-lesson survey as neutral or below, with that group encompassing 70% of our results. The ones who answered agree or above make up the last 30% of students. We were unable to confirm how much knowledge they actually had before our lesson due to time constraints.



**FIGURE 2.** Pre-Lesson survey results of both classes

By analyzing the post-lesson survey results in Figure 3, which asked the same question, we can notice that in both classes there are no longer any students who answered below neutral.

In the hands-on class, we can see that 13% of the students rated their understanding as neutral, compared to the 9% in the hands-off lecture. The hands-off lecture had 59% of students state that they were comfortable with the subject matter compared to the 50% in the hands-on. As far as strong understanding goes, the hands-on class reported more concrete understanding with 37% strongly agreeing to the question, while 32% reported the same in the hands-off lecture. One important thing to note is that the class sizes were different, so the difference in data percentages could have been caused by that varying amounts of participants.



**FIGURE 3.** Results of the Post-Lesson Survey for both classes.

## CONCLUSIONS

Looking at these results, we can recognize that both hands-on and hands-off classes helped the students understand cybersecurity topics. It is interesting to note that the hands-on class seemed to have more students that said that they strongly agreed to the statement “I am comfortable with cybersecurity topics”, while the hands-off had more on the neutral and agree responses. We believe that this is due to the fact that as students advance into the cybersecurity field, the material becomes much more intensive, so the students in the hands-on class that understood the subject understood it better than those in the hands-off, but for some students, it was harder to keep up due to the increased difficulty.

Overall, this project demonstrates that both ways of teaching the information have their own benefits, with the hands-on approach seeming to increase knowledge by a larger amount when the students can keep up, and the hands-off being better for a wider range of interest / academic ability. For future research, we would like to do this with more than two classes, create an actual test to access knowledge instead of just a survey, and attempt a follow up test as well to see if the students retain knowledge better one way compared to the other.

Additionally, as a result of this project, we believe that the high school teacher community is in dire need of simple and yet instructive cybersecurity examples and hands-on activities that could be introduced as part of the general computer science curriculum. The goal of such activities would be to make students aware that cybersecurity careers exist (for instance, through CyberSeek [8]), what resources are out there, and what high school students can do now to prepare themselves for an abundance of opportunities that exist in the cybersecurity field. The cybersecurity activities, assignments, and exercises could be developed by undergraduate students as part of their research work and shared with the community via GitHub [9], TeachCyber [10], and other online resources.

## REFERENCES

1. C. Ventures, “Cybersecurity jobs report 2018-2021,” <https://cybersecurityventures.com/jobs/>.
2. V. Barr and C. Stephenson, “Bringing computational thinking to k-12: what is involved and what is the role of the computer science education community?” *Inroads* 2, 48–54 (2011).
3. B.-Å. Lundvall, *National systems of innovation: Toward a theory of innovation and interactive learning*, Vol. 2 (Anthem press, 2010).
4. A. R. Korwin, R. E. Jones, *et al.*, “Do hands-on, technology-based activities enhance learning by reinforcing cognitive knowledge and retention?” *Volume 1 Issue 2 (spring 1990)* (1990).
5. P. Chapman, J. Burket, and D. Brumley, “Picoctf: A game-based computer security competition for high school students,” in *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)* (2014).
6. Hak5, “Rubber ducky;” (), <https://shop.hak5.org/collections/usb-rubber-ducky>.
7. Hak5, “Wifi pineapple;” (), <https://shop.hak5.org/products/wifi-pineapple>.
8. CyberSeek, “Hack the gap: Close the cybersecurity talent gap with interactive tools and data,” <https://www.cyberseek.org/>.
9. GitHub, “Development platform inspired by the way you work,” <https://github.com>.
10. TeachCyber, “Education is the first line of defense,” <https://teachcyber.org/>.