

Creating a Digital Literacy Curriculum for Students in Morocco

An Interactive Qualifying Project
submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
degree of Bachelor of Science

by
Patrick Bailey
Kaley Du
Ethan Reed
Kavya Mani
gr-rabat23-DigitalLiteracy@wpi.edu
<https://sites.google.com/view/mo23-digi/home>

Date:
4 May, 2023



WPI



Educall
L'éducation autrement ... !

Report Submitted to:

Prof. Bland Addison

Prof. Fabio Carrera

Prof. Joseph Doiron

Worcester Polytechnic Institute

And to:

Dr. Yassine Ettayal
Educall

This report represents the work of WPI undergraduate students submitted to the faculty as evidence of completion of a degree requirement. WPI routinely publishes these reports on its website without editorial or peer review. For more information about the projects program at WPI, please see <https://www.wpi.edu/academics/undergraduate>

Abstract

In Morocco, the percentage of the population that has access to the internet has risen from practically 0% in 2000 to almost 90% in 2021. Because of this rapid increase, a much larger portion of the population has become vulnerable to the internet's inherent dangers due to a lack of widespread digital literacy education. Educall is an educational social enterprise that wants to create a digital literacy curriculum that could teach Moroccan students how to be safe online, which our team constructed and evaluated. We first determined the main internet threats plaguing Morocco by talking with parents and teachers, and we worked with Educall to design a curriculum to teach about each of these issues. Our resulting curriculum contains five modules: Misinformation, Personal Information, Social Media & Mental Health, Cyberbullying, and Malware. Each module was tested and evaluated using pilot programs, one with primary school students and the rest with high school students, the latter being done fully virtually. Each module was determined to be very successful in terms of student satisfaction, but although students believed they learned a lot, more testing and formal evaluation should be performed to determine the true educational content. Our major recommendations include instituting formal pre- and post-evaluations to determine the curriculum's teaching effectiveness, as well as to provide more time for teaching every module. We hope that Educall will be able to use this curriculum to spread digital literacy education to students throughout Morocco.

Acknowledgments

This project could not have been nearly as successful as it was if not for the support of our collaborators.

We would like to begin by thanking Educall, specifically Dr. Yassine Ettayal (CEO of Educall) and Mohamed Benhsain (Project Coordinator) for being understanding, cooperative, and friendly liaisons to work with, going above and beyond at every possible opportunity. They were incredible mentors in designing the major deliverable of this project, and they provided us with all of the resources we could possibly desire to schedule interviews with teachers, events with parents, and pilot programs with students. They were always enthusiastic about helping in every way they could, and we couldn't have asked for better sponsors to facilitate this project.

We would also like to thank Vision School for providing us such a wonderful space to work in, and for allowing us to both observe their classrooms and take class time to run a pilot program with our curriculum. Vision School's teachers and parents were major assets to building the foundations of this project, and we greatly appreciate that they took the time to talk to us.

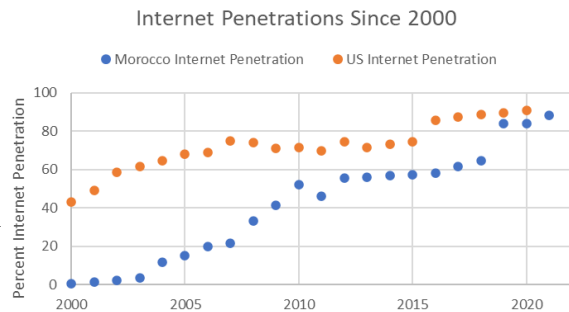
We are also very grateful to the students from DigiGirlz and Vision School for being willing and active participants in the pilot programs we ran of the curriculum. They were great to work with, and their input and involvement in the lessons were invaluable to the refining of our curriculum.

Finally, we are appreciative of our advisors Professors Bland Addison, Fabio Carrera, and Joseph Doiron for constantly being supportive at every point in the project. Their consistently helpful advice and guidance were instrumental to the quality of this project, and it would not have been nearly as complete or refined without their support.

Lastly, we would like to thank WPI for providing us with the opportunity to experience Morocco and work on this project with such wonderful people in such an amazing location.

Executive Summary

Internet access is rapidly expanding across Northern Africa. In Morocco, the percentage of the population who have access to the internet has risen from practically 0% in 2000 to almost 90% in 2021. Although the spike in access is beneficial, it brings all of the internet's various threats with it. Citizens need to learn the skills needed to combat these threats, especially young people that use the internet the most, but the current system for teaching these skills is inadequate. Our sponsor Educall aimed to confront this lack of education by assisting us in constructing a curriculum that can teach digital literacy to Morocco's students. Our group researched the dangers that accompany internet access, conducted interviews with teachers and conversations with parents to determine the most relevant digital literacy topics, designed the digital literacy curriculum, ran pilot programs to evaluate it, and recommended and implemented changes to make it as effective as possible.



Many online threats trouble Africa's population today. Morocco's web space is rated by multiple cybersecurity companies to be among the least safe in the world in terms of malware site prevalence (Reboot 2022; Kaspersky 2021), there are very few studies examining cyberbullying that nonetheless conclude the rate of cyberbullying is high - over 50% at a Moroccan primary school (Miami et al. 2020), and another study found that 50% of Moroccan students do not use strategies to discern misinformation on the internet from real information (Mrah & Tizaoui 2018). These high rates of vulnerability to internet threats indicate that young Moroccans are highly in need of developing digital literacy skills. Through our research, we developed a definition of *digital literacy* that consists of five main components: critical thinking and evaluation, internet safety, uploading and sharing content, internet etiquette, and understanding the risks of social media. We aimed to create a curriculum that addresses these five subjects, as well as teaching about the internet's various threats.

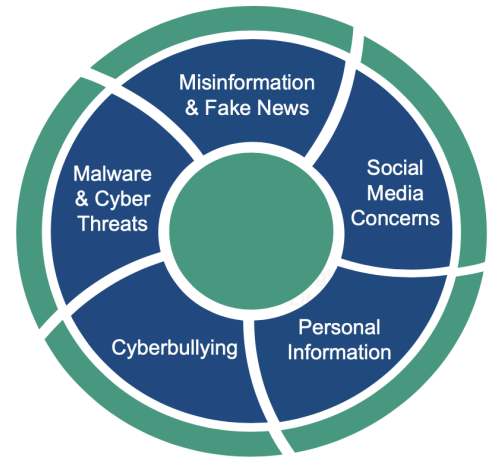
This project's three main objectives were to:

1. Determine Digital Literacy Needs
2. Design a Digital Literacy Curriculum
3. Evaluate the Curriculum

We first reviewed the literature and determined the most relevant internet threats: Misinformation, Personal Information, Social Media Safety & Mental Health, Cyberbullying, and Malware. We then held semi-structured interviews with 6 teachers, as well as holding informal conversations with 6 parents during a parent's day event, to allow us to organize these topics in order of importance based on the responses of both groups (sorted above in order of

decreasing importance to parents and teachers). The interviews with teachers also provided insights into Vision School and the types of activities that would interest students most. With these topics of focus identified and ranked, we were able to design the curriculum around them.

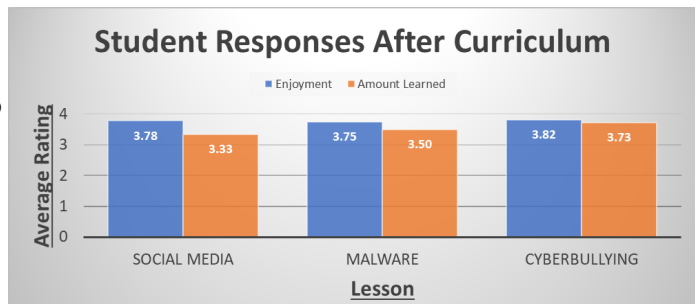
Our curriculum was split into five modules to address each one of the five internet threats. Each module consisted of a six-piece structure: the goal and objectives, required time and materials, introduction, lesson content and activities, assessment, and conclusion. When designing the lesson content, it was crucial that we created activities fostering an interactive and engaging atmosphere. We observed several classes taught by Educall’s Mohamed Benhsain to examine how Educall accomplished this ideal, and we modeled our own activities to encourage the same type of student participation achieved in Educall’s pedagogy.



For the assessment portion, we created pre- and post-evaluations to give before and after the pilot, respectively, to gauge the students’ increase in knowledge. We also developed a satisfaction survey that consisted of a few questions asking about student enjoyment, how much the students thought they learned, and feedback for improving the lesson. We asked Educall to review the module drafts and provide suggestions to make them more engaging, and we implemented their feedback.

Finally, we were able to evaluate the curriculum by running pilot programs for each module. We were able to invite Vision School’s 3rd and 4th graders to a pilot of one module, and we invited high school and college aged students from DigiGirlz for the rest of the pilots. Overall, the pilots revealed that every module of the curriculum worked very well. Students demonstrated that they really enjoyed and felt like they learned a lot in every lesson. However, we were not able to collect enough data from the pre- and post- evaluations to make concrete conclusions about the educational value of the curriculum.

Because of that, our recommendations for improving the curriculum further include instituting better methods to encourage participation in the evaluations, as well as allowing more time for each module than was allotted for the pilot programs. The content in some of the modules can also be modified slightly to add more information about the topics students are interested in. With these recommendations, Educall will be able to continue improving the digital literacy curriculum. We are confident that Educall



can use this curriculum to teach countless students about internet safety in the future, helping not only students, but teachers and parents for years to come.

Authorship

<u>Section</u>	<u>Written By:</u>	<u>Edited By:</u>
Abstract	Kaley Du	Patrick Bailey
Acknowledgements	Patrick Bailey, Kavya Mani	Patrick Bailey
Executive Summary	Ethan Reed	Kaley Du
1. Introduction	Patrick Bailey, Kaley Du	Kaley Du, Patrick Bailey
2. Background	Patrick Bailey	Kavya Mani
2.1 Access to the Internet in Morocco	Patrick Bailey	Kaley Du
2.1.1 Internet Diffusion in Morocco	Patrick Bailey	Kaley Du
2.1.2 Social Media in Morocco	Ethan Reed	Kaley Du
2.2 Internet Threats	Patrick Bailey	Kavya Mani
2.2.1 Internet Threats in Morocco	Patrick Bailey	Kavya Mani
2.2.2 Social Issues and Cyberbullying	Kaley Du	Patrick Bailey
2.2.3 Scamming and Malware	Patrick Bailey	Kavya Mani
2.2.4 Misinformation	Kavya Mani	Kaley Du, Patrick Bailey
2.3 Digital Literacy in Moroccan Education	Patrick Bailey	Kavya Mani
2.3.1 What is Digital Literacy	Kavya Mani, Patrick Bailey	Kaley Du
2.3.2 Education System and Digital Literacy in Morocco	Kaley Du	Patrick Bailey
2.4 Educall, Vision School, and DigiGirlz	Kavya Mani, Kaley Du	Kaley Du, Kavya Mani
2.5 Best Practices for Curriculum Design	Kaley Du	Patrick Bailey

2.5.1 Working with the Community	Kaley Du	Patrick Bailey
2.5.2 Effective Curriculum Structure and Content	Kaley Du	Patrick Bailey
2.5.3 Activities to Increase Engagement	Kaley Du	Patrick Bailey
2.5.4 Knowledge Assessment	Kaley Du	Patrick Bailey
3. Methodology	Patrick Bailey, Kaley Du	Kavya Mani
3.1 Determine Digital Literacy Needs	Kaley Du, Patrick Bailey	Patrick Bailey
3.2 Design the Curriculum	Patrick Bailey	Patrick Bailey, Kaley Du
3.2.1 Material to Teach	Patrick Bailey	Patrick Bailey, Kaley Du
3.2.2 Teaching Methods	Patrick Bailey	Patrick Bailey, Kaley Du
3.2.3 Teacher Feedback	Kaley Du	Patrick Bailey
3.2.4 Constructing the Evaluation Method	Kaley Du	Patrick Bailey
3.3 Pilot Programs: Evaluating the Curriculum	Patrick Bailey, Kavya Mani	Patrick Bailey
4. Results and Analysis	Patrick Bailey	Kaley Du
4.1 Digital Literacy Needs	Kaley Du	Patrick Bailey
4.1.1 Background Information from Teacher Interviews	Kaley Du	Patrick Bailey
4.1.2 Results from Teacher Interviews About Areas in Need	Patrick Bailey	Kaley Du
4.1.3 Curriculum Feedback from Teacher Interviews	Kaley Du	Patrick Bailey

4.1.4 Digital Literacy 4 Parents Day Results	Kaley Du	Patrick Bailey
4.2 Designed the Curriculum	Patrick Bailey	Kaley Du
4.2.1 The Activities in Each Module	Patrick Bailey	Kaley Du
4.3 Evaluation of the Digital Literacy Curriculum	Patrick Bailey	Patrick Bailey
4.3.1 The First Pilot- Misinformation	Kavya Mani, Kaley Du	Patrick Bailey
4.3.1.1 Misinformation Pilot - 3rd Grade	Kavya Mani, Kaley Du	Patrick Bailey
4.3.1.2 Misinformation Pilot - 4th Grade	Kavya Mani, Kaley Du	Patrick Bailey
4.3.1.3 Misinformation Pilot Feedback and Recommendations	Kavya Mani	Patrick Bailey
4.3.2 The Second Pilot - Social Media Safety & Mental Health	Kaley Du	Patrick Bailey, Kavya Mani
4.3.2.1 Social Media Pilot Pre-Evaluation Findings	Kaley Du	Patrick Bailey
4.3.2.2 Lesson on Social Media Safety and Mental Health	Kaley Du	Patrick Bailey
4.3.2.3 Social Media Pilot Post-Evaluations	Kaley Du	Patrick Bailey
4.3.2.4 Recommendations for the Social Media Module	Kaley Du	Patrick Bailey
4.3.3 The Third Pilot - Malware	Patrick Bailey	Kavya Mani
4.3.3.1 Malware Pre-Evaluation Findings	Patrick Bailey	Kavya Mani
4.3.3.2 The Malware Lesson	Patrick Bailey	Kavya Mani

4.3.3.3 Feedback and Final Recommendations for Malware Module	Patrick Bailey	Kavya Mani
4.3.4 The Fourth Pilot - Cyberbullying	Kavya Mani	Patrick Bailey, Kaley Du
4.3.4.1 Cyberbullying Lesson	Kavya Mani	Patrick Bailey, Kaley Du
4.3.4.2 Feedback and Recommendations for Cyberbullying Module	Kavya Mani	Patrick Bailey, Kaley Du
4.3.5 The Fifth Pilot - Personal Information	Ethan Reed	Patrick Bailey, Kaley Du
4.3.5.1 Personal Information Lesson	Ethan Reed	Patrick Bailey, Kaley Du
4.3.5.2 Personal Information Activities and Conclusion	Ethan Reed	Patrick Bailey, Kaley Du
4.3.5.3 Personal Information Results and Post-Evaluation Analysis	Ethan Reed	Patrick Bailey
4.3.5.4 Recommendations for Personal Information Module	Ethan Reed	Patrick Bailey, Kaley Du
5. Conclusion and Recommendations	Patrick Bailey, Kavya Mani	Patrick Bailey, Kavya Mani

Table of Contents

1 Introduction	11
2 Background	13
2.1 Access to the Internet in Morocco	13
2.1.1 Internet Diffusion in Morocco	13
2.1.2 Social Media in Morocco	16
2.2 Internet Threats	17
2.2.1 Internet Threats in Morocco	18
2.2.2 Social Issues and Cyberbullying	19
2.2.3 Scamming and Malware	20
2.2.4 Misinformation	21
2.3 Digital Literacy in Moroccan Education	21
2.3.1 What is Digital Literacy	22
2.3.2 Education System and Digital Literacy in Morocco	23
2.4 Educall, Vision School, and DigiGirlz	25
2.5 Best Practices for Curriculum Design	26
2.5.1 Working with the Community	26
2.5.2 Effective Curriculum Structure and Content	26
2.5.3 Activities to Increase Engagement	28
2.5.4 Knowledge Assessment	29
3 Methodology	30
3.1 Determine Digital Literacy Needs	31
3.2 Design the Curriculum	31
3.2.1 Material to Teach	32
3.2.2 Teaching Methods	32
3.2.3 Teacher Feedback	33
3.2.4 Constructing the Evaluation Method	34
3.3 Pilot Programs: Evaluating the Curriculum	34
4 Results and Analysis	35
4.1 Digital Literacy Needs	35
4.1.1 Background Information from Teacher Interviews	35
4.1.2 Results from Teacher Interviews about Areas in Need	36
4.1.3 Curriculum Feedback from Teacher Interviews	37
4.1.4 Digital Literacy 4 Parents Day Results	38
4.2 Digital Literacy Curriculum	39
4.2.1 The Activities in Each Module	40
4.3 Evaluation of the Digital Literacy Curriculum	43

4.3.1 The First Pilot - Misinformation	43
4.3.1.1 Misinformation Pilot - 3rd Grade	43
4.3.1.2 Misinformation Pilot - 4th Grade	45
4.3.1.3 Misinformation Pilot Feedback and Recommendations	46
4.3.2 The Second Pilot - Social Media Safety & Mental Health	47
4.3.2.1 Social Media Pilot Pre-Evaluation Findings	47
4.3.2.2 Lesson on Social Media Safety & Mental Health	48
4.3.2.3 Social Media Pilot Post-Evaluations	51
4.3.2.4 Recommendations for the Social Media Module	54
4.3.3 The Third Pilot - Malware	55
4.3.3.1 Malware Pre-Evaluation Findings	55
4.3.3.2 The Malware Lesson	57
4.3.3.3 Feedback and Final Recommendations for Malware Module	59
4.3.4 The Fourth Pilot - Cyberbullying	60
4.3.4.1 Cyberbullying Lesson	60
4.3.4.2 Feedback and Recommendations for Cyberbullying Module	61
4.3.5 The Fifth Pilot - Personal Information	62
4.3.5.1 Personal Information Lesson	62
4.3.5.2 Personal Information Activities & Conclusion	67
4.3.5.3 Personal Information Results and Post-Evaluation Analysis	68
4.3.5.4 Recommendations for Personal Information Module	70
5 Conclusion and Recommendations	70
References	72
Appendices	77
Appendix A. Internet Penetration Rates of Selected Countries	77
Appendix B. Function of Common Malwares	78
Appendix C. Surveys	78
Appendix C1. Survey for Students	78
Appendix C2. Survey for Teachers	80
Appendix D. Interview Questions	82

1 Introduction

Internet access is rapidly expanding across Northern Africa. In Morocco, the percentage of the population that has access to the internet has risen from practically 0% in 2000 to almost 90% in 2021. This digital expansion has allowed Moroccans to access the incredible wealth of information and connections the internet has to offer. However, the internet also comes with many new risks and dangers, such as those associated with social media (cyberbullying, addiction, mental health, etc.), and the presence of malware, internet scams, and misinformation throughout the web.

Although Morocco's internet access has increased rapidly, it has not been able to develop enough educational resources to teach the public about the internet's threats. In fact, Morocco's internet space is consistently ranked as one of the most dangerous in the entire world (Reboot 2022; Bischoff 2022), and Morocco has a high rate of cyberbullying occurrence with few efforts to confront the problem compared to the United States and other countries (Zhu et al. 2021; Miami et al. 2020). In the only published study examining cyberbullying in Morocco (at this time, May 2023), 54.5% of respondents reported being involved in cyberbullying, which is a very high statistic, and another study found that 60% of surveyed Moroccan middle schoolers showed an inability to distinguish between fact and opinion online (Miami et al. 2020; Mrah & Tizaoui 2018). Internet problems such as these are exacerbated by the fact that parents and teachers are also unknowledgeable in internet safety, with 78% of parents not being sufficiently informed in protecting their children online and only half of them feeling like they can respond appropriately to their children being cyberbullied (Latrech 2022). As a result, the people living in Morocco, especially youth who use technology the most, need the skills to navigate the internet and all of its complexities safely, also known as digital literacy (Statista 2022). Digital literacy has many definitions, but our definition contains five major components: critical thinking and evaluation, internet safety, uploading and sharing content, internet etiquette, and understanding the implications of social media. These categories are complex in practice, and some ideas and issues can fit into multiple categories, but these categories encapsulate the best definition of the term. Because of the rapid increase in internet access and all of its accompanying problems, there is not yet a firm infrastructure for teaching children the digital literacy skills to safely navigate the internet and its various dangers.

Educall, a Rabat-based company partnered with several schools and programs for students, aims to fill the gap in Moroccan children's knowledge of digital literacy. Educall is a social enterprise founded by Dr. Yassine Ettayal in 2015 with the goal of bringing education to all children regardless of gender, social class, and economic status. They highly value making education more interactive and engaging, including by using gamification and a learn-by-doing approach to create a fun and interactive learning process. Moreover, efforts by the government and other agencies are beginning to address these problems, including the Generalization of ICTs (information and communication technologies) in Education (GENIE) program, the Moroccan

Emergency Plan for Higher Education (UNESCO 2022; Nfissi 2013), and the more recent “Digital Generation” project being implemented by the Digital Development Agency (ADD). The GENIE program focused on expanding the use of ICTs in public schools, and the Moroccan Emergency Plan for Higher Education introduced Media Studies and Cyber Culture into the curriculums of English, Arts, and Humanities departments at universities (UNESCO 2022; Nfissi 2013). However, GENIE was more focused on increasing access to ICTs than teaching skills and best practices for using them, and the Media Studies and Cyber Culture course is limited to universities rather than being available to the majority of the public (Hanae 2019). The “Digital Generation” project seeks to establish a National Training Plan in the Digital Field in Morocco in order to encourage innovation and strengthen human capital (ADD); this project is spread across multiple organizations and has material that teaches both parents and teachers and younger kids. However, we still need to support this movement with a full curriculum for younger students that can be taught in person or online in an interactive session. This creates a need for a curriculum focused solely on digital literacy that is far more accessible to all levels of students.

For this project, we partnered with Educall to create a digital literacy curriculum for students 9-17 years old. We first determined which areas were most in need by conducting literature searches, interviewing teachers, and conversing with parents. These areas were determined to be Misinformation, Personal Information, Social Media & Mental Health, Cyberbullying, and Malware, in order of decreasing importance. We then designed the curriculum with five modules to cover each of the five areas in need, using other successful curriculums as models and considering advice from teachers and Educall. Finally, we evaluated the curriculum by running several pilot programs with student participants from the DigiGirlz program and the Vision Primary School in Rabat, analyzing how engaging it is and how effective its lessons and activities are for teaching. These programs showed us that the curriculum as a whole is very enjoyable, and that students feel like they learned a lot, but more testing will be required to numerically verify its effectiveness. Although the curriculum seemed overall effective, we also provided some recommendations for adjusting each module of the curriculum based on our own experiences teaching it and on participant suggestions. We believe that this curriculum is highly effective for teaching students the vital digital literacy skills they need, and that with more testing and minor adjustments, it will be a valuable asset to help Educall teach Moroccan children to be safe online.

2 Background

In order to learn how to best design and implement our digital literacy curriculum, we researched relevant topics including internet access in Morocco, types of online threats, digital literacy education in Morocco, and best practices for curriculum design. We first examined how access to the internet in Morocco has grown in the past couple decades, and how widespread various aspects of the internet are in the culture. We also researched all of the various threats that can be seen on the internet and their prevalence in Morocco, which led us to our definition of digital literacy. Finally, we looked into how digital literacy is currently taught in Moroccan schools, and the external efforts pushed by the government and other organizations that aim to increase knowledge about digital literacy, including why they are not as effective as desired. In examining these efforts, we discovered some important patterns in effective, engaging, and interactive curriculum design, which we aimed to implement into the curriculum we design.

2.1 Access to the Internet in Morocco

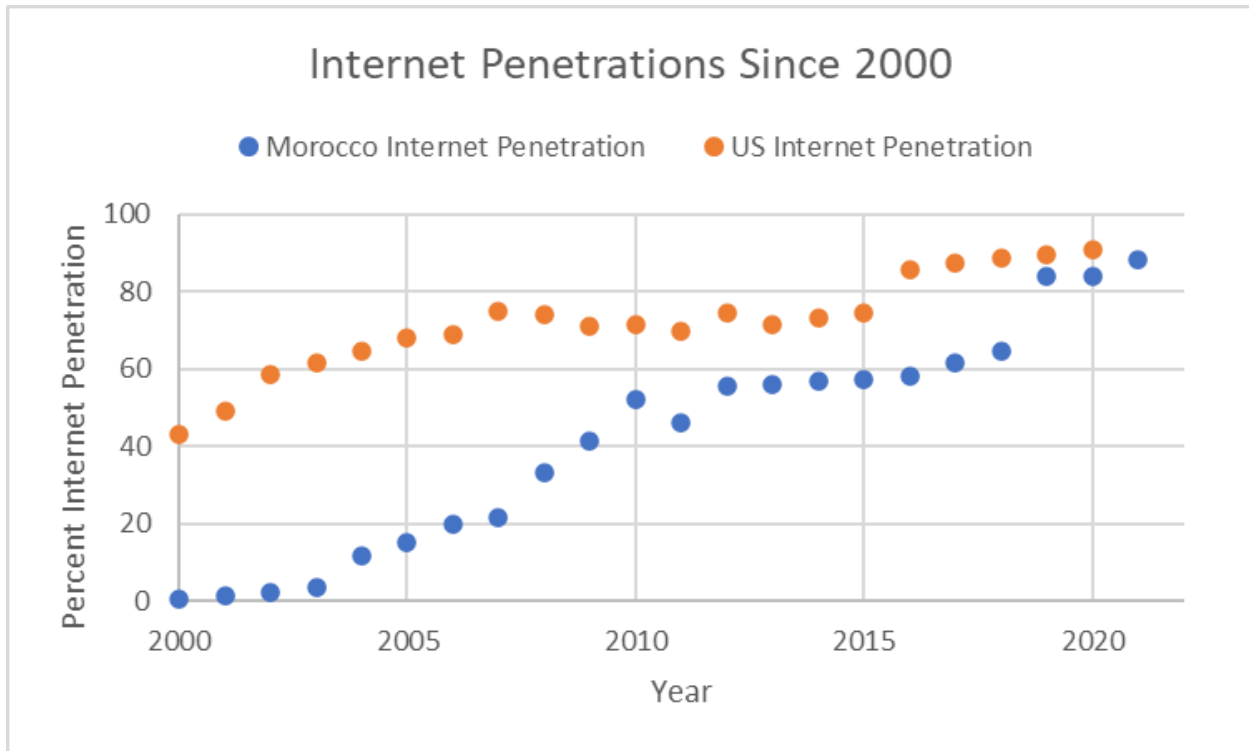
Morocco's internet access has skyrocketed, leaving a gap in knowledge and understanding about the internet between the generations that have now grown up with it and their parents and teachers who did not. This section describes the recent increase in internet access in Morocco over the past couple decades, especially compared to the United States, discusses the sources from which Moroccans obtain internet access, and evaluates the social media usage patterns of Moroccans.

2.1.1 Internet Diffusion in Morocco

The internet is a very useful and powerful resource that provides access to near unlimited information and connections to others, and has become an essential part of living in the modern age. As such, high speed internet access is expanding across the globe, which is measured by the internet penetration rate. This statistic represents the percentage of a population that has access to the internet, and a graph of this statistic per country (with a population above 50,000 people) as of July 2022 is shown in Appendix A. As can be seen, almost every developed country in the world has an internet penetration rate of close to 100%, which shows a clear relation between the level of access a country has to the internet and how developed the country is.

Recently, Morocco's internet penetration rate has rapidly increased, as shown below in Figure 1.

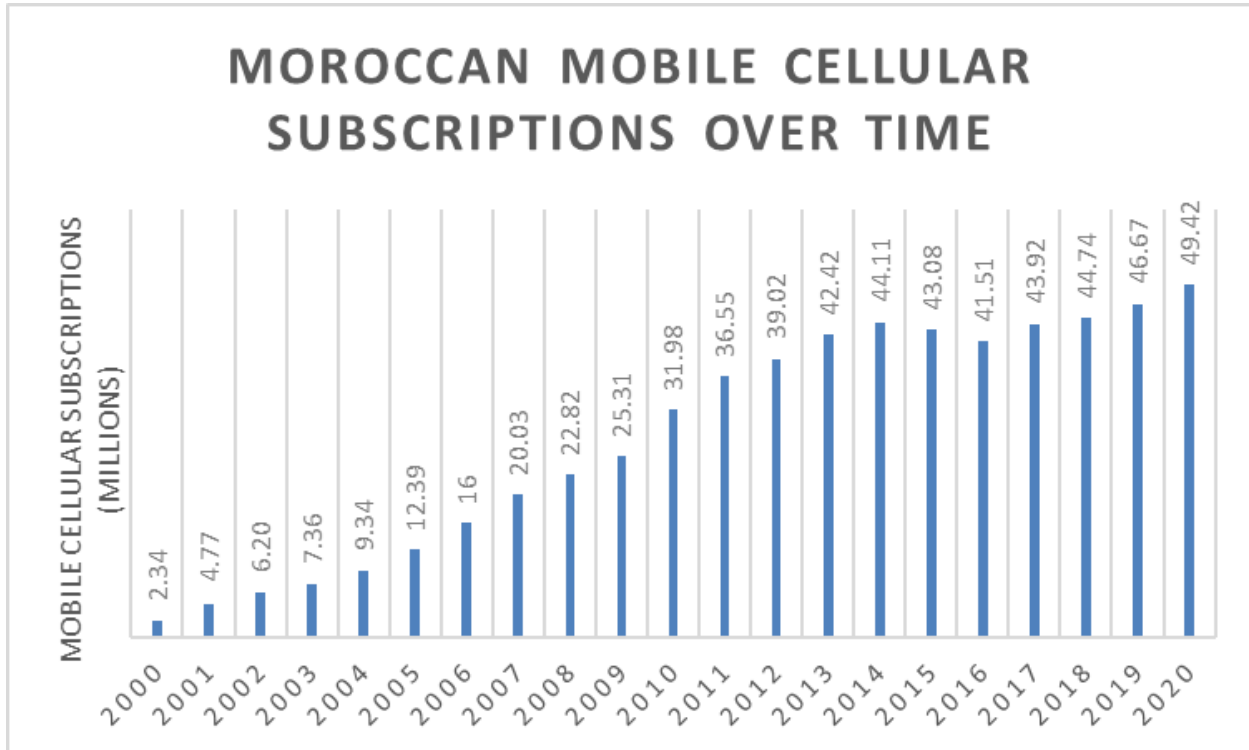
Figure 1: *The increases in internet penetration in the US and in Morocco from 2000 to 2021*



Note. Internet penetration refers to the percentage of the population that used the internet in the last three months. As can be seen, within the last 25 years, Morocco’s internet penetration rate has gone from almost 0% to being on par with the United States at around 90% (*Individuals using the internet, 2021*).

From 2000 to 2021, the US’s internet penetration doubled, from about 43% to about 91%. Meanwhile, in the same time period, Morocco’s internet penetration has grown by a multiple of almost 62, from about 0.7% to about 88%. This massive jump in internet accessibility in Morocco has left a corresponding gap between generations. Children and adolescents today have grown up with the internet, while their parents, teachers, and other authority figures have not developed an understanding of it, and are oftentimes left unable to effectively teach their children how to safely use it. This insufficiency leaves these children vulnerable to the various threats that come with the internet, such as cyberbullying, misinformation, and privacy risks, as well as a lack of guidance regarding the usage and applicability of the internet in everyday life. Another indicator of the increase in access to digital information is the cellular subscription growth over time, shown below.

Figure 2: *The rise in cellular subscriptions in Morocco from 2000 to 2020*



Note. Above contains the number of cellular subscriptions in Morocco from 2000 to 2020, in millions of sales (Taylor 2023).

As access to cell phones has risen, so has access to the internet. Cellular subscriptions in Morocco have increased by almost 25 times, from 2.34 million to 49.42 million, since 2000. This further created a barrier between generations, as older people do not see a need to adopt these new tools, exacerbating the problems created by this gap.

However, despite this increased access across the country, rural access lags behind. Rural residents constitute 37.1% of the overall population, yet most rural residents do not have access to phone lines and high speed internet (Ibahrine, M. & Zaid, B 2016). As a consequence, those in rural areas have less experience with technology and digital literacy. Another study was performed by the Moroccan government to determine how students handled the switch to remote learning during the peak of Covid. It found that 83.5% of students did not keep up with their lessons in remote learning, including 79.1% of urban students and 94.6% of rural students (Amdil 2021). The main causes of these large numbers are the general ineffectiveness of online teaching on such short notice created by the pandemic, but also due to lack of access to consistent, high speed internet. A study involving Moroccan university students found that 53.3% were challenged in remote learning by slow internet access, and another 26.7% had no internet access (Mouaziz et al. 2023). This data indicates that although most people in Morocco have access to

the internet, the quality of the internet is not consistent and the internet as a platform is not reliable for a large number of Moroccans. This problem is even worse for rural students, as there are many areas that are too poor to afford strong internet access, and there are some areas where providers don't even offer this access. Some rural Moroccan students had to walk very long distances to access a place with good enough internet for remote school learning, and some were forced to stop going to school because their families could not afford strong enough internet, or providers did not reach far enough into rural areas (Amdi 2021). Overall, this data about remote learning during Covid shows that although almost all of the population has access to the internet, the access is not equal throughout the entire population, and in many places it is not reliable enough for people to view it as a useful tool.

2.1.2 Social Media in Morocco

Morocco, despite only gaining widespread internet access rather recently, has increased its online presence greatly in the past two decades. *Morocco – Global Digital Insights* stated that Morocco's internet users already encompasses 84% of their total population (31.59 million users), with a 1.2% increase between 2021 and 2022 (363,000 people), leaving a mere 16% (5.96 million people) yet to access the internet in early 2022. Internet speeds grew by 6% last year with fixed speeds increasing by 50%, meaning that even though Morocco already has a deep stake in digital technology, it still has room to grow and is successfully doing so.

Regarding social media in particular, in the beginning of January 2022, roughly 63% of the population used social media (23.8 million people), which increased about 8% (1.8 million users) between 2021 and 2022.

Table 1: *Individual social media platform usage statistics in Morocco*

Platform	Number of Users (Account Age Requirement)	Ad Reach of Total Population	Ad Reach of Eligible Population	Male to Female Audience Percentage
Youtube	21.4 million (13+)	67.7%	57%	51% / 49%
Facebook	18.95 million (13+)	50.5%	65.5%	37.8% / 62.2%
Instagram	9.3 million (13+)	24.8%	32.1%	54.1% / 45.9%
Tiktok	5.97 million (18+)	23.1%	23.1%	52.7% / 47.3%
Snapchat	5.5 million (13+)	14.6%	19.0%	31.6% / 68.4%
LinkedIn	3.5 million (18+)	11.1%	9.3%	65.5% / 34.5%
Twitter	2.85 million (13+)	7.6%	7.6%	56.4% / 43.6%

Note. Above shows the individual social media platform specifics of the number of users, ad reach of total population, ad reach of eligible population (those older than the minimum age for using the service (often 13 years old)), and male to female audience percentage throughout Morocco by early 2022 (Kemp 2022).

2.2 Internet Threats

Despite all of the internet’s great uses, it also gives people a platform to prey on those that are not capable of navigating it safely. These threats can be divided up into three categories:

1. Social Issues
2. Virus and Personal Information-Related Threats
3. Misinformation

Social issues involve those that occur because of unsafe usage of social media or other user-connecting services, including events like cyberbullying, inappropriate interactions from or towards others, social media addiction, the mental health effects caused by social media, and the “digital footprint” left behind by users.

The virus infection and personal information-related threats include malware and other software unwittingly downloaded onto a device, cyber attacks such as phishing, denial of service (DoS and DDos) attacks, and account hacking.

The misinformation category includes threats caused by writers manipulating their audience by drawing fallacious conclusions, ignoring relevant information or overemphasizing it, misrepresenting or falsifying statistics, and maliciously or ignorantly manipulating people's thoughts and emotions through propaganda and unrealistic threats. These ideas will all be further defined and discussed in this section.

2.2.1 Internet Threats in Morocco

Digital literacy and internet safety are crucial skills to have in the modern age, and there are many dangers to users who cannot protect themselves. These threats are especially relevant in Morocco, which was recently ranked the eighth most dangerous country for browsing the internet (Rahhou 2022). Rebootonline, a market research company, found that Morocco has 500 phishing sites and 1000 malware-hosting sites per 100,000 URLs, 1603 compromised computers per 100,000 users, and 19 drive-by downloads (accidental downloads of malware) per month per 100,000 URLs (Reboot 2022). They also found that almost 23% of mobile users in Morocco suffered a malware attack, with only 8% of users responding that they have an antivirus software installed (Rahhou 2022). This lack of precaution is especially concerning because Moroccans have a high risk of encountering danger and seem relatively nonchalant about maintaining their safety, which leads to many Moroccans falling victim to cyber attacks that they may not know how to deal with. Additionally, Kaspersky, an antivirus software company, published a study of how many Kaspersky users were subjects of web malware attacks. They found that Morocco held the eighth highest risk of online infection among participating countries, at a risk of 18.87%. This study further proves how comparatively dangerous Morocco's webspace is to other countries, and why digital literacy is crucial in protecting the population (Kaspersky 2021). The specific dangers of browsing the internet will be detailed in the next section, but it is clear that the lack of internet safety practices currently being used by the Moroccan population poses a huge risk to internet users.

Additionally, Morocco, like the rest of the world, has fallen victim to the issue of **cell phone addiction**, and its accompanying anxiety and withdrawal symptoms. A study was performed asking teenagers about their smartphone and social media habits (specifically Facebook, being the most popular platform), their experiences with cell phone addiction symptoms, anxiety, and nomophobia (fear of being separated from their cell phone), and their general school performance (Louragl et al. 2019). The researchers ultimately concluded that a rise in cell phone addiction was correlated with a decrease in concentration and school performance, and that there is a definite correlation between cell phone addiction and anxiety (Louragl et al. 2019). Another study found that 57% of surveyed students in Morocco were developing symptoms similar to addiction, and more than half of them had experienced negative effects from social media on their job, relationship or studies, health and well-being (Alaika et al. 2020). This shows that social media may have a wide hold over Moroccans, and is causing

negative effects in many aspects of their lives. The anxiety caused by cell phone dependence is clearly a huge issue, both for Morocco and the world, but the fact that this technology has so rapidly spread throughout Morocco means that a lot of children and adolescents are likely entirely unaware of this issue.

Studies have also been performed aiming to evaluate how well equipped the population of Morocco is at thinking critically about what is seen online. One study, performed by Mrah and Tizaoui, found that 50% of Moroccan students do not use strategies for evaluating the legitimacy of information found on the internet, with more than 60% of students expressing an **inability to distinguish between fact and opinion** (Mrah & Tizaoui 2018). Additionally, 68% of survey takers expressed that social media was the most credible source of news, followed by online news sources with 28% of responses (Mrah & Tizaoui 2018). These high numbers imply that students in Morocco are extremely vulnerable to fake news, information, and propaganda, and do not employ skills to verify the information that they see on the internet. In fact, the same study found that 88% of respondents had never received training in digital literacy skills (Mrah & Tizaoui 2018). If such a high number of Moroccan students view social media as the most credible source of news without even beginning to question the quality of the information received, they are vulnerable to being manipulated by the writers of the information, which is worsened by the presence of **terrorist organizations** actively recruiting in Morocco. Terrorist organizations tend to use social media to spread propaganda due to how quickly it will circulate on the internet, how cheap it is to produce, and how little risk there is to spread it. In fact, ISIS alone was known to produce as many as 90,000 posts on social media every day (Lieberman 2017). Because of how rarely Moroccan children verify information they find online, and on social media in particular, they can easily be preyed on by terrorist organizations, and are vulnerable to being manipulated by dangerous information they find online.

2.2.2 Social Issues and Cyberbullying

There are also many other aspects of social media and online interactions that can pose threats: sharing personal information and being enticed to meet strangers in person, social media's deleterious impact on mental health including through cyberbullying, soliciting inappropriate content and interactions, and social media addiction, and malicious use of digital footprint. Social media can impact a user's mental health by painting better pictures of other people's life than reality. Through photoshopping pictures and advertising products, an influence can present false narratives about how a person's life should look. Social media addiction can cause negative effects similar to any other kind of addiction, including negatively impacting work, creating tensions in personal relationships, and jeopardizing one's health. **Cyberbullying** is bullying through the internet, whether through text messages, videos, calls, or other forms of media. According to a study in a Moroccan primary school in Rabat, 54.5% of students reported being a perpetrator of cyberbullying, a victim of it, or both (Miami et al. 2020). This study was

also one of the first of its kind in Morocco, which emphasizes how this problem is not understood very well within Morocco and that there is a need to educate about it (Miami et al. 2020). A person's **digital footprint** is the information each person leaves on the internet, and it can never be entirely erased. **Inappropriate content and interactions** also exist or can occur, so it is important to be aware of it, especially for younger audiences, and to establish general *netiquette* - etiquette on the internet - to avoid spreading such content. These sorts of dangers with social media are only rarely discussed, especially not by social media companies, so it is vital to share this information to protect users from the potentially damaging effects of social media.

2.2.3 Scamming and Malware

There are many threats that an internet user may encounter, either from malicious websites or programs, fake communications, hostile users collecting information they should not have, or a combination of the three. **Malicious programs** are known as malware, and they can have a variety of negative effects. Some examples of this are ransomware, spyware, adware, computer worms, rootkits, scarewares, and keyloggers, whose functions are detailed below in Appendix B (Baker 2023). The easiest way to address these threats is through **antivirus software**, which will recognize a user's unknowing download of malware or visit to an unsafe website and block threats before they occur. Antivirus softwares are also able to read files on a computer and isolate and remove infected software (Jefferson 2023). The second threat is known as phishing or spoofing, in which attackers send malicious communications in hopes of baiting a user into downloading malware, clicking a malicious link, or giving away personal information. These sorts of nefarious activities are most often done through email, text messages, or social media, but can also be done over the phone (Baker 2023). Attackers can also target account information and passwords in order to gain access, which makes it important to use strong passwords that are not reused across accounts and to use multi-factor authentication to verify one's identity (Jefferson 2023).

Additionally, many internet users in Morocco rely on public wifi, which leaves them vulnerable to mass phishing and malware attacks directed at every connected user, as well as man-in-the-middle (MITM) and packet sniffing attacks (Zaharia 2023). **MITM attacks** allow a malicious user to intercept any information sent through the network, including passwords, emails, and other sensitive information, collect it, and even modify it before sending it to the intended recipient. **Packet sniffing attacks** are more passive, but also result in the malicious user being able to collect information sent through public, unsecure networks (Zaharia 2023). The best way to protect against these kinds of attacks is to use a virtual private network, or VPN, which will automatically encrypt any data sent through a network, leaving any malicious user collecting only meaningless junk.

There are also other techniques that attackers can use against businesses specifically, such as **denial-of-service** (DoS) and **distributed DoS** (DDoS) attacks, which overwhelm a website or software with many fake “users” so that real users cannot connect, but these attacks that target businesses are outside of the scope of our curriculum (Baker 2023). Because there are so many unique threats that users need to guard against, it is important that users have a strong digital literacy education to protect themselves.

2.2.4 Misinformation

There are numerous sources online that spread false information, intentionally or not, which can influence the audience. **Misinformation** is accomplished when not all facts and perspectives on a topic are shared, or when statistics are misrepresented or made up entirely. For example, a lot of African national statistics in education and health are misleading due to systemic bias in administrative data systems. One study found that many African schools exaggerate their enrollment in their official data, with schools supposedly having up to one-third higher enrollment number than was established in survey results (Glassman & Sandefur 2014). **Falsified or misleading statistics** are everywhere because of how easy it is to create and manipulate them, and it is crucial that people have the ability to verify them. “Fake news” is another problem often discussed by news sources, but it is difficult for the audience to determine what qualifies as fake news or misinformation. The skill to determine what information is misinformation in the news is known as “news literacy”, defined as “the ability to critically analyze news content” (Bonnet, & Rosenbaum 2020). Being able to analyze a source of information and understand how and why it is presented the way it is is critical to being able to understand a complex topic from multiple points of view. There are various strategies that can help with analyzing resources, such as verifying the author, the date, the news site, reading through the original sources of statistics, and finding other sources of information about the topic to establish a complete perspective. Throughout the world, misinformation is a massive problem, as it can both mislead individuals and have large scale effects across society as a whole, so it is important for everyone to have the skills to think critically about information circulated online.

2.3 Digital Literacy in Moroccan Education

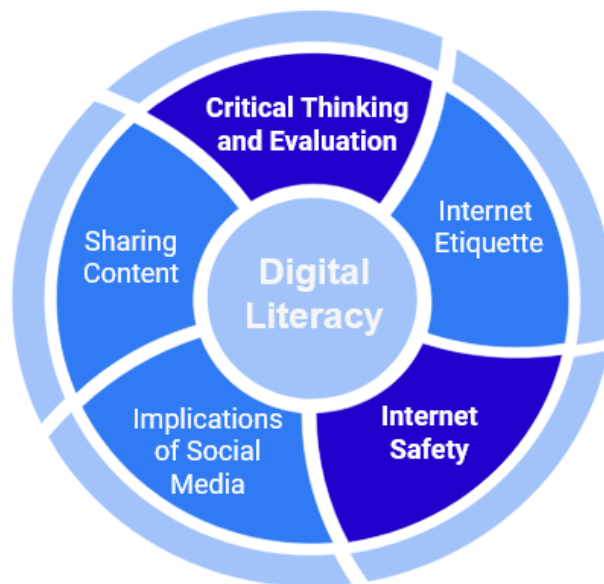
This section will discuss what digital literacy means for the purposes of this project in Moroccan elementary schools and also the extent of digital literacy being taught in these schools. It will also examine current efforts to increase the digital literacy of Moroccan students by both the government and by other businesses, which corresponds to the objectives of this project.

2.3.1 What is Digital Literacy

Digital literacy is a topic whose importance is becoming increasingly recognized, and its history has become very extensive. The term *digital literacy* was only recently coined; people often used to encompass digital literacy practices into computer literacy. Computer literacy focuses more on how to use the various aspects of computer functionality, while digital literacy is directed towards the best manner in which to engage intellectually with these functionalities (Buckingham 2015). With so much of the world interacting with the internet as a daily practice, learning about how to best behave while using it has become arguably more important than learning basic functional skills. As computers move from a mere tool into an essential part of life, the need to explore digital literacy as a standalone concept arises.

There are many definitions for what digital literacy is since digital literacy covers a large scope of topics and ideas. As stated above, we established its five main components: critical thinking and evaluation, internet safety, uploading and sharing content, internet etiquette, and understanding the dangers that social media creates. These categories are complex, and many concepts can overlap between them, but the skills within them encompass the entirety of our definition of digital literacy.

Figure 3: *Definition of Digital Literacy*



Note. The chart above displays our definition of digital literacy, which includes the responsible sharing of content, understanding the possible dangers of social media, and other aspects of internet safety, as well as internet etiquette. Critical thinking and evaluation are also

vital skills for everyone to have in every area of internet and computer use. We believe the highlighted topics, *critical thinking and evaluation* and *internet safety*, are the areas most in need of development among Moroccan students.

Critical thinking is vital to confront the flood of information found on the internet since it is very easy for anyone to post anything, regardless of truthfulness. Internet etiquette allows users to converse with others in respectful and safe ways. Internet safety skills are important so that a user's livelihood is not threatened by malicious users and programs online. Social media is especially prevalent currently and understanding its safe usage and its potential harms is crucial for an internet user. Finally, the responsibility that comes with sharing content is an important principle to accept so that a user does not unintentionally harm others.

2.3.2 Education System and Digital Literacy in Morocco

Digital literacy is not incorporated into the official Moroccan curriculum effectively. In a survey of middle school teachers, the majority said it is not taught at all to students, though there may be efforts among some educators to teach it (Hanae 2019). These teachers affirmed that traditional educational subjects are more typical, and the typical curriculum does not allocate time to digital literacy education at all. This neglect of digital education handicaps students in responding to current dangers presented by the internet and makes them ill-equipped to work with the internet professionally (Hanae 2016). In the curriculums that do teach digital literacy, **media is often treated as unfamiliar and dangerous**, rather than a useful tool that can have some negative effects for unaware users. Because of its potential for harm, education focuses on “the negative aspects of media and popular culture and on sensitizing [students] to the best way to avoid its threat” (Hanae 2019). This fosters an attitude of avoidability that does not help students develop critical thinking skills or learn to analyze what they inevitably come across on the internet. Due to the increasing scope of the internet, it is safe to say that almost all young people will gain access to the internet, but may not be equipped with the tools and skills to safely navigate it.

The government does understand how important it is to teach digital literacy, as there have been multiple governmental programs to help spread the use of digital technologies in education. One significant program from Morocco is **Généralisation des TIC dans l'Enseignement** (GENIE, Generalization of ICTs in Education), launched in 2005, which had a goal to extend information and communication technologies (ICTs) in public education. This program ensured that Digital Literacy would be taught to educators through training sessions or online platforms, and would be taught to children through either introducing ICT as a subject or through integrating it into other subjects (UNESCO 2022). Originally meant to be a 3 year program, the effort is still ongoing, with new directives and additions being added. However, one study found that the program is not as effective as intended, which is further complicated by the

fact that the program has a lack of administrative support or follow-up visits after completion of its training (Ismaili 2020). In the wake of such scrutiny, it is unclear whether the digital literacy education provided is sufficient.

Another program, the **Moroccan Emergency Plan for Higher Education**, was introduced in 2009, which brought Media Studies and Cyber Culture into the curriculums of English, Arts, and Humanities departments (Nfissi 2013). These courses teach students about media and how it works, and aim to help them understand its impact on society. As part of the curriculum, students are taught media literacy, including how to think critically about messages promoted in media, how to detect manipulation, how to view sources with opposing opinions, and how to use media for sustainable development and positive outcomes. Students are also taught information literacy, which consists of “library skills, computer literacy, critical-thinking skills, visual literacy and culture literacy, in addition to research skills and evaluation of print and online sources” (Nfissi 2013). However, these subjects are restricted to only students studying English, rather than being a requirement for all students, which greatly limits the number of people that benefit from learning these skills.

There have also been a few global forums held on the issue of digital literacy, most notably the **First International Forum on Media and Information Literacy** held in collaboration with the United Nations Educational, Scientific and Cultural Organization in the Sidi Mohamed Ben Abdellah University, Fez (UNAOC 2011). It resulted in many resolutions towards improving Media and Information Literacy in Morocco, including a World Media and Information Literacy Week. However, most of these measures are more focused on global effects than specific to Morocco (Nfissi 2013).

Currently, the **Digital Development Agency (ADD)** is implementing a “Digital Generation” project that seeks to establish a National Training Plan in the Digital Field in Morocco in order to encourage innovation and strengthen human capital (ADD). Several organizations are involved in this effort. One such organization is Academia Raqmya, a national e-learning platform with various courses focusing on digital skills. These courses are completely online, and feature multi-year programs that target employees of public administrators, companies such as startups, and the general public. There are two main courses: “Digital Improvement” for public administrators and employees and “Digital Acculturation,” which focuses on raising awareness and educating the general public on digital skills (ADD). Another company that supports the ADD’s project is E-himaya, who created a website that includes resources to help teach children about various digital topics and internet safety. It features guides and resources for students, parents and teachers (ADD). With these resources, a parent could make a profile to teach their children techniques to safely use the internet and spread awareness of all the internet’s risks (ADD).

On a non-governmental level, one organization that helped tackle the issue of teaching digital literacy is **Simsim Participation Citoyenne**, an independent Moroccan organization that seeks to increase citizens’ roles in public decision making through technology while also helping governments respond better to citizens’ demands (Parliamentwatch Network 2023). This

organization helped create a portal known as Salam@, which includes a step-by-step digital safety guide and many articles covering different aspects of digital safety. They also host workshops. This initiative is the first step, and it is important to continue development in this area of education, especially targeted towards children.

Overall, the attitude towards teaching children more about digital literacy is positive, especially among teachers. In one study surveying teachers about teaching digital literacy in secondary school, the respondents most commonly believed that integrating these topics was important (Hanae 2019). Teachers seem to have more robust and substantial knowledge in digital literacy than students. For example, in another study, many teachers knew different ways to check if a source is credible, while students rarely did (Mrah & Tizaoui 2018). This discovery means that many teachers are able and willing to teach this material, given the opportunity. The opinion towards teaching digital literacy in schools is positive, but until the government or schools can place it into their curriculums or effective external resources become available, the need for teaching these skills will not be fulfilled (Mrah & Tizaoui 2018; Hanae 2019). All in all, though there is some recognition of the importance of digital literacy among Moroccans, the amount of skills taught and applied is insufficient, so the efforts to teach digital literacy must be increased.

2.4 Educall, Vision School, and DigiGirly

Educall, or Education for All, was founded in 2015. It is an educational social enterprise whose vision is to ensure the development and fulfillment of Moroccan children regardless of their social class, as well as to simplify the learning process and make it fun and interactive through gamification techniques and technology (Educall). Educall adopts a systemic approach to involving different members of the educational ecosystem: children, parents, teachers, educators, and educational institutions. Recently, they have seen the developing need for digital literacy education for Moroccan students, and have begun work to develop programs to teach students how to stay safe online.

Vision School is a primary school in Rabat, Morocco. This school prides itself on its trilingual environment, providing students the opportunity to learn a new language, English, at a young age through an immersion learning environment. When a student joins Vision School at a preschool age, they continue to learn maternal languages throughout the higher grades, including English and Arabic. French is also taught to a level of conversational proficiency. Vision School uses an innovative approach to education, with specially trained staff, an exclusive education program, and a simulation environment that was inspired by the Canadian Vision model.

DigiGirly is a program with a goal of female empowerment in STEM. This program pairs up high schoolers with university level mentors and involves extensive hands-on

experiences and a mix of in-person and digital technology workshops and activities for girls (DigiGirlz).

2.5 Best Practices for Curriculum Design

By looking at past successful curriculums, one can derive some components that make them effective. Firstly, working with the target community to design the curriculum is vital because it allows the curriculum to be best tailored to the community's needs and interests. Past curriculums also show that including engaging activities is crucial for learning, and that knowledge assessments following a lesson are useful for both reminding people what they just learned and for examining how well the curriculum taught its content. The examples presented here provide many best practices for building a useful and engaging curriculum.

2.5.1 Working with the Community

In preparing educational courses meant for Morocco and other developing countries, programs have shown that ample research, interaction with the community, and working with local people are vital for success. A pilot education from the **Wikimedia Foundation**, first launched in 2020, contextualized teaching materials by searching literature, conducting teacher surveys and interviews, and consulting the community. This program involved local Wikimedia affiliates, which were selected through a transparent selection process. Since this took place during the COVID-19 pandemic, Moroccan teachers were individually addressed to participate, and their participation was self directed (Patnaik 2020). The outcomes for the Wikimedia Foundation course were relatively positive, as a majority of participants agreed that the course helped them demonstrate improved media and information literacy competencies. This emphasizes the importance of working closely with the local population to determine what works best.

2.5.2 Effective Curriculum Structure and Content

There are a lot of patterns that can be seen in effective curriculums, such as how many are split into three or four modules, each covering a general category, with topics varying between different curriculums. One curriculum made by the **Secdev Foundation**, based in Canada but working throughout North Africa, uses a particularly good framework. This curriculum is known as **CyberSTAR**, and it features a design using a six-branched star, each representing a main topic. Each session of a course starts with an overview of the topic and a way to get students invested in why it is important, followed by discussions and activities

regarding the topic, then some time to wrap up and review everything learned (The Secdev Foundation 2022). Most often, the general topics covered by a digital literacy curriculum include safety, security, the idea of a digital footprint, appropriateness of posting online, password safety, and reliability of sources. They are often split by age range, with each range covering slightly different topics (The Secdev Foundation 2022; Common Sense; Windham School District).

CyberSTAR has topics that include visuals in both the form of Powerpoint slides and as a teacher's guide (The SecDev Foundation 2022). It covers **six main topics**: data, conversations, digital identity, digital risks, passwords, and devices (The SecDev Foundation 2022). These topics discuss digital risks, including how online users can unknowingly download malware, and data and conversations covering the importance and steps to securing important data, whether personal or confidential corporate files, as well as keeping private correspondence on digital media. Their presentation of digital identity also has information that can help support the section of our curriculum dealing with social consequences of media, as it covers the digital footprint as well as social media safety and privacy. The teacher's guide includes the required materials, appropriate handouts, and quizzes, along with an outline of the course content. It lists the main subheadings of topics and activities, as well as the intended length of each one. This curriculum guideline provides a loose framework which teachers can work with, not requiring a particular order, so that they can best tailor it to their classrooms (The SecDev Foundation 2022).

UNESCO has a **Media and Information Literacy Framework** that can serve as a guideline for digital literacy courses all around the world (Wilson et al. 2011). This framework has 9 core modules, as well as 2 non-core modules and 3 non-core units, the most relevant to the curriculum being developed by this project being internet opportunities and challenges and information literacy and library skills. The course can be implemented as stand-alone, integrated into another course, or hosted online; the curriculum gives space for improvisation and experimentation with multiple formats (Wilson et al. 2011).

Simsim Participation Citoyenne's Salam@ web portal has four main categories: fundamentals of digital safety, phone protection, safe communication and digital identity. It provides many specific guides under each category, such as public computer safety tips, the importance of having antivirus software, and how to install one. These guides provide visuals along with step-by-step tutorials for certain technologies. They also cover the psychological effects of the internet and try to spread awareness about it.

All in all, most of these curriculums include visual resources such as Microsoft Powerpoint slides and a general agenda for teachers to follow. They all seem to be rather loosely constructed, which allows teachers and others learning from them to use them at their own pace and to teach in ways more specific to their own needs.

2.5.3 Activities to Increase Engagement

Interactive elements in education, such as discussions and games, are important to maintain interest in the material, especially for younger students, and in general bring better understanding of content. The UNESCO Media and Information Literacy Curriculum for Teachers highlights a few main pedagogical techniques used in effective teaching (Wilson et al. 2011). The *Issue-Enquiry approach* is student-centered and focuses on issues in contemporary society and implements problem-solving and decision-making through inquiry stages. *Problem-based learning* is highly structured and cooperative, and focuses on solving real-life problems. *Scientific enquiry* utilizes an enquiry cycle to explore an issue in the same way a scientist would. There are also case studies, which focus on a single event, cooperative learning, textual analysis of various media genres, contextual analysis, translations into different forms of media, simulations of students in a certain role, and production, which entails learning by doing. These pedagogies can be used to help generate valuable activities that are both interactive and engaging (Wilson et al. 2011). Some example activities from this curriculum include having students google themselves, writing a “letter to the editor” about the importance of the internet, looking at the news to analyze it for bias and analyzing movies, drawing a diagram relating information, information society, ICTs and media information literacy, and writing an essay and creating a Powerpoint presentation on how recent technology is changing how information is generated and used.

Many curriculums incorporate **discussions** into class time, using topics that connect to **daily struggles or experiences** many students have encountered in their own lives. These can be linked to a different topic, and the relation can make the content more engaging. Some curriculums also include handouts, which include information students can review during and after class. The CyberSTAR curriculum implemented activities that help students practice digital literacy in real time. For example, pertaining to the category of malware, students are directed to change their privacy settings on social media or are given phishing emails they must determine are fake (The SecDev Foundation 2022). Classes also utilized various outside websites, tools, and resources that help demonstrate digital risk, such as the Trace My Shadow website, which helps students view their digital footprint and gives tips based on what kinds of technology they use (The SecDev Foundation 2022). Curriculums focusing on younger audiences focus on ways to make the process more interactive and fun for younger kids. In a curriculum for K-12 for Common Sense Education, another activity is to create a comic of a “digital citizenship superhero” who spots and fixes a scenario of bad digital citizenship (Common Sense). Other activities include being given websites and determining if they are reliable or not (Standerford 2020).

The Wikimedia Foundation course found that the most effective lessons included high quality contextualized assets and increasing reach using large scale partnerships (Patnaik 2020). In addition to asynchronous digital materials, synchronous training sessions were held so that teachers could ask questions, demonstrate processes, and explore elements. Facebook groups

were also created as spaces to share answers to prompts or activities, as well as post questions (Patnaik 2020). Local coordinators also identified guest speakers to participate in training sessions (Patnaik 2020).

Good **visuals** and other audio and video resources are important. The resources from the E-himaya website aimed towards kids utilize animations, sound, and a robot mascot “Nabih” to help convey its lesson topics (ADD). This added flair can help keep kids engaged and assist them with understanding concepts better. It has three main sections: the library, video library and quiz section (ADD). The library includes multiple digital guides that educate on digital safety topics and include graphics that help convey topics. The videos convey information in a different format. The quiz features quick explanations for each correct and incorrect answer, and can serve as a learning exercise in itself. The guides for parents include exciting and colorful visuals as well. This shows how important it is to make a visually fun and engaging curriculum for kids (ADD).

These curriculums have shown that using class discussions relevant to the students’ lives, various game-like activities, and outside interactive websites and tools are essential aspects to creating an engaging curriculum.

2.5.4 Knowledge Assessment

To assess how effective a course was, many curriculums also included **post-session assessments**. CyberSTAR included post-class quizzes that assess the knowledge covered in each module. They also had quizzes for more challenging or specific topics, such as how to spot a phish (The SecDev Foundation 2022). The Wikimedia Foundation utilized website metrics to measure the amount of views on trainings, engagement with activities, and the amount of completions to gauge success (Patnaik 2020). The e-himaya website has a quiz portion as well that can also serve as a learning activity. Evaluation of the effectiveness of courses can be really important for both reminding learners about what they just learned as well as gauging how effective the course was in teaching its content.

3 Methodology

For this project, we partnered with Educall to develop a curriculum that can fill the existing gaps in Morocco's digital literacy knowledge, providing knowledge of the internet's various threats and some best practices to avoid them. To do this, we interviewed teachers and talked to parents to determine the **major internet threats** they were concerned with, we **designed and refined our curriculum** using modern teaching practices and techniques to boost student engagement, and we **ran pilot programs** of every module of our proposed program and analyzed its success.

We mainly worked with Educall and the Vision Primary School in Rabat, with some input from other teachers and educational professionals from the United States. Our spatial boundaries were limited to Vision School in Rabat and the electronic platform we used to communicate with students from the mentorship program DigiGirlz. One of our pilot programs was hosted with the 3rd and 4th graders at Vision School, while the rest were hosted virtually with students from DigiGirlz.

Figure 4: Map of area surrounding Vision School



Our major objectives, written below, will be expanded on in the following sections.

1. Determine Digital Literacy Needs
2. Design a Digital Literacy Curriculum
3. Evaluate the Curriculum

3.1 Determine Digital Literacy Needs

In order to tailor our curriculum to the needs of the community, we first determined what digital literacy topics needed the most focus. We accomplished this through literature reviews, interviews with teachers, and informal conversations with parents.

We used **semi-structured interviews**, with questions shown below in Appendix D, as the primary method to gather information from Educall and Vision School's teachers. These interviews were all recorded with participant permission. Most of them were conducted in English since most teachers spoke it fluently, but some had a translator from Educall present to facilitate communication. These interviews focused on which areas of digital literacy teachers thought were most relevant or missing from the current educational system, as well as whether our lesson plans could be used to teach effectively. To analyze these interviews, we drew patterns of certain keywords and ideas, and especially focused on areas of need within the current digital literacy curriculum.

We and Educall also asked parents about their childrens' and their own broader knowledge of digital literacy at a **digital literacy networking event**. The event aimed to inform **parents** about our project and about resources produced by other companies to teach digital literacy to children. In short, informal conversations, we asked parents about their opinions on the various digital literacy topics that we aimed to teach, including what they felt was most important for their children to learn. This data was used to determine what to focus on most in the curriculum, and gave us a very small idea about what the greater population of Morocco feels is relevant in digital literacy.

3.2 Design the Curriculum

As we researched how a curriculum should be designed and what topics Moroccan teachers and parents thought were relevant, we constructed and developed a prototype. Each curriculum consisted of the goal and objectives, time needed and materials, introduction, lesson content and activities, assessment and conclusion. The curriculum was designed with the ideals we learned from past curriculums in mind; we wanted to make sure it would suit the community well, that it was fun, engaging, and interactive for the students, and that there was an evaluation

included in it to help students better remember the lesson. We then asked for feedback from teachers and Educall in interviews, which was used to further refine the curriculum.

3.2.1 Material to Teach

There were five major areas that we determined were most relevant after our research and what we learned from teachers and parents:

1. Misinformation
2. Personal Information
3. Social Media Safety & Mental Health
4. Cyberbullying
5. Malware

In order to maximize the simplicity of the curriculum, we divided the curriculum into **five modules**, each one addressing one of these focus areas. The Misinformation module teaches some best practices for appraising information, such as determining the writer's intent and biases, and how easy it is to spread fake news online. The Personal Information module aims to teach about the dangers of spreading sensitive information online and discusses ways to protect one's privacy and personal information. The Social Media Safety & Mental Health module discusses how to act safely on social media, including keeping personal information off social media, judging and addressing inappropriate content and interactions, some general netiquette skills, and some potential impacts of social media on mental health such as social media addiction. The Cyberbullying module teaches students what cyberbullying looks like, the impacts it can have, and gives some best practices for addressing cyberbullying. The Malware module teaches about different types of malware and how to avoid downloading them. We proposed to use various methods to teach all of these topics, including many activities and scenarios, and some methods of evaluation for each subject.

3.2.2 Teaching Methods

Prior to designing activities for the curriculum, we observed two of Educall's classes, one with 4th graders and one with 2nd graders. We aimed to examine the atmosphere of the lesson to understand how Educall hosted classes following their own ideology for student interaction in classrooms. We shared Educall's goal in making education as engaging and fun as possible throughout the project, and with that goal in mind, we brainstormed a list of **interactive activities** that can be applied to our content. This list is shared below.

1. Have the class as a whole **brainstorm a concept map** about a particular idea
2. Have the class form smaller groups to **discuss a scenario** or open-ended question
3. Have students find and present answers to questions to the entire class, then have a class discussion
4. Have students **move around the classroom** to indicate responses to questions
5. Quiz students by posing **open ended scenarios or stories** and asking them to determine the best course of action
6. Present caricatures of misinformation and ask students to brainstorm ways to **verify that it is misinformation**
7. Students group up and simulate a team game show similar to Family Feud or Jeopardy
8. Have students **construct their own posters** or other artistic activity
9. Use food or toys to represent concepts, or have students think of ways to represent concepts using them
10. Have students analyze a scenario or story and point out what a character did well or poorly
11. Give students a hypothetical person's or their own personal information (Zip code, school name, first and last name, address, etc) and **have them find that person on the internet**
12. Have students and educators **play pictictionary or charades** to act out concepts
13. Teach children to **use outside websites and tools** that help evaluate security and digital footprint

These activities were expanded after teacher interviews, then matched with topics that they best fit after reviewing the results of our interviews with Educall and with teachers. In making lesson plans based upon these kinds of interactive activities, we hoped to make them both engaging and educational for our students.

3.2.3 Teacher Feedback

As we constructed our curriculum, we showed Educall's teachers the preliminary drafts of the modules we had developed and asked them to give feedback to improve the curriculum. These responses allowed us to go back and evaluate the curriculum further, making more adjustments to increase its effectiveness.

3.2.4 Constructing the Evaluation Method

The lessons also all had some type of **evaluation** built into them. Each module - except Cyberbullying - includes multiple choice questions that can be administered both before and after the completion of the lesson to compare the change in the students' knowledge. The Cyberbullying module, being more experiential than factual by nature, evaluates students' knowledge through discussion and responses to scenarios and stories. These evaluations allowed us to establish a form of measurement to determine whether the lessons were effective.

3.3 Pilot Programs: Evaluating the Curriculum

Finally, in order to test how effective our curriculum is and to gain feedback on how to improve it, we ran several **pilot programs**. We worked with several groups of students including the 3rd and 4th graders from Vision School as well as high school and university students from the DigiGirlz program, both with parental permission. For the pilot program with Vision School's students, we taught the Misinformation module, and we were aided by staff from Educall to prepare the environment and teach the curriculum, with a team member co-facilitating the lesson. This pilot took place on April 12th at the Vision School, and the duration of the lesson was 45 minutes. There were two pilot events run with the DigiGirlz students, taking place on April 20th and April 24th, and they were run with the help of Educall virtually using Google Meet. The Social Media & Mental Health module and the Malware module were run concurrently on April 20th, with students being able to switch between the lessons as they desired. The Cyberbullying module and the Personal Information module were run concurrently on April 24th, also allowing students to switch between the lessons. Each of these DigiGirlz pilots ran for about 1.5 hours, after a 10 minute introduction of the curriculum development project.

As each pilot program proceeded, we had one team member teach as the other members observed the classroom and students, **taking notes** to determine what went well and what went poorly. In the DigiGirlz pilots, we used two team members for each module, one teaching and the other taking notes. We recorded what occurred during the session and noted which activities were **most effective**, which ones retained **less student attention**, and whether any instructions were **unclear or confusing**. Afterwards, students and educators who participated in the pilot were surveyed in order to give their thoughts on how the lesson went. Prior to some of the lessons, the student participants were given the pre-evaluation quiz asking them to assess their knowledge on the topics we aimed to teach, and afterwards were given the post-evaluation. These notes and evaluations were analyzed, and improvements to the curriculum were recommended and implemented immediately. This pilot program allowed us to see our curriculum in action, which gave us very useful information to improve it further.

4 Results and Analysis

The major objectives for this project were to **determine the areas of digital literacy** most in need to be covered by a digital literacy curriculum, to **design the curriculum** around these needs, and to **evaluate the curriculum's** effectiveness. We first determined the areas of digital literacy most in need by reviewing the literature and through talking with teachers and parents, which were ranked in order of decreasing importance: Misinformation, Personal Information, Social Media & Mental Health, Cyberbullying, and Malware. We then designed the curriculum around these topics, taking into account the conclusions we drew while analyzing past curriculums and making sure to implement the best practices into our curriculum. Finally, we tested each module of the curriculum through pilot programs. The pilot of the Misinformation module was run with both the 3rd and 4th graders at Vision School, while the rest were run virtually with the high school and college students involved with DigiGirlz. Every module of the curriculum was determined to be very enjoyable and engaging for the students, but although it appeared that students retained a lot of what they were taught, we were not able to collect enough data to make concrete conclusions about the educational value of the curriculum.

4.1 Digital Literacy Needs

In order to determine what digital literacy needs were most urgent and how we should tailor our curriculum to them, we needed to consider our stakeholders; **teachers, students, and parents**. We first studied the literature to create a list of the most relevant internet problems worldwide, then we **interviewed six teachers** and **talked to six parents** at a digital literacy networking event to determine which areas deserve the most focus. In order of decreasing importance, we determined the topics to be organized as Misinformation, Personal Information, Social Media & Mental Health, Cyberbullying, and Malware.

4.1.1 Background Information from Teacher Interviews

We **interviewed six** of Vision School's teachers, with one person asking the questions while the other took notes, and recorded each session. Through our teacher interviews, we discovered that teachers know that subjects in our curriculum are **important to teach about**, but that there is **no official framework** for teaching these subjects in the current curricula. When asked what they think digital literacy is, most teachers responded that it was related to how to use technology and the internet, some mentioning it was about awareness and staying safe. A few

teachers mentioned that they hadn't thought of it much before the interview or until recently, but recognize its importance. Others already had topics such as cyberbullying brought up in their classes through observation and discussion and addressed them as they surfaced; one teacher brought up how at times they would stop the class in order to discuss such a topic. There is also a "wake up your brain" session at Vision School where students discuss various topics, including topics of technology and digital literacy. Many teachers allow students to use certain software and web pages, but don't allow students to venture beyond what they are provided; a consequence of not getting the chance to teach critical thinking skills pertaining to the internet. As no official course has been run about these topics, and their importance is acknowledged, this further cements a goal in helping teachers teach such subjects.

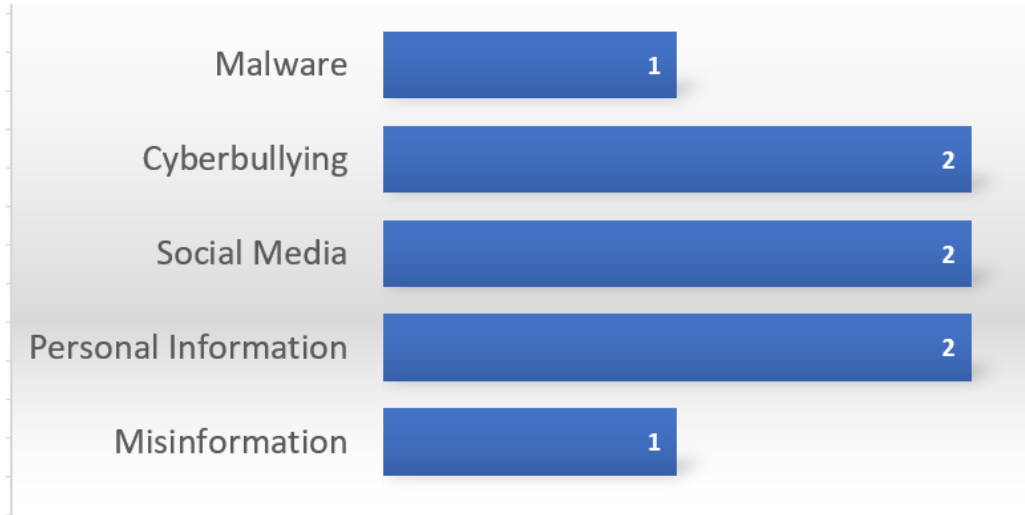
Teachers have observed the students' exposure to the internet and social media. They spoke about the fact that students **use video streaming platforms** like YouTube, Tiktok and Twitch, and they frequently have had students come up to them and ask questions, such as what a PS5 is. When one teacher tried to show a video and an ad popped up, the students were able to **recognize it as inappropriate**. That teacher also mentioned how some kids were being exposed to content inappropriate for their age on YouTube, such as subjects related to sexual education that are not talked about in a proper or necessarily correct way. Although most teachers said their students generally consumed content on social media and didn't post, one teacher mentioned a student who was trying to get people in her class to follow her on instagram. Despite these exposures to the internet, a teacher mentioned how **students are often forbidden** from using the internet at home and are not taught anything about it, which in turn makes the students more curious and means eventually they eventually discover the internet on their own but are ill-equipped to stay safe and avoid internet threats. These interviews gave us a baseline of how students learn about the internet and even gain access to it, but don't use it much and are kept in the dark about a lot of its aspects, including how it can be dangerous or misleading.

4.1.2 Results from Teacher Interviews About Areas in Need

Within the interviews with teachers from Vision School, we asked about what areas of digital literacy they felt their students were lacking. As shown below in Appendix D1, we asked teachers about the relative comfort level of the students and the school with each of the five topics that we concluded were relevant and necessary to teach. They unanimously stated that all five of the topics are very important, and that they could not think of anything else that should be added alongside them. This response was taken to mean that our curriculum contains all the relevant topics within digital literacy, without any topic being unnecessary. We then asked them to rank our five topics by importance. Counting each of the teacher's top two rankings as one vote, **Personal Information**, **Social Media**, and **Cyberbullying** each had two votes, followed by Misinformation and Malware with only one vote each, as shown in Figure 5. This implies that these teachers deem personal information safety, social media safety, and cyberbullying to be the

most relevant at Vision School, which allowed us to target these pieces of the curriculum for development.

Figure 5: *Teachers' Most Prioritized Topics*



4.1.3 Curriculum Feedback from Teacher Interviews

The results from our interviews with teachers influenced the content we would cover in our curriculum, and how we would teach it. The stories about kids using social media and potentially learning inappropriate or dangerous information from it confirmed that Moroccan kids at Vision School are **familiar with social media**, which gave us more incentive to teach students about social media. Multiple teachers discussed that since students are going to use the internet on their own, they would want the students to be able to discern what's reliable on their own, so we gave our Misinformation module more priority. A teacher also told us a story she heard about students accessing the dark web, and learning about the Blue Whale Challenge, a dangerous internet challenge that asks participants to comply with increasingly violent demands. We added some content to the personal information and social media modules that address this problem in a general way.

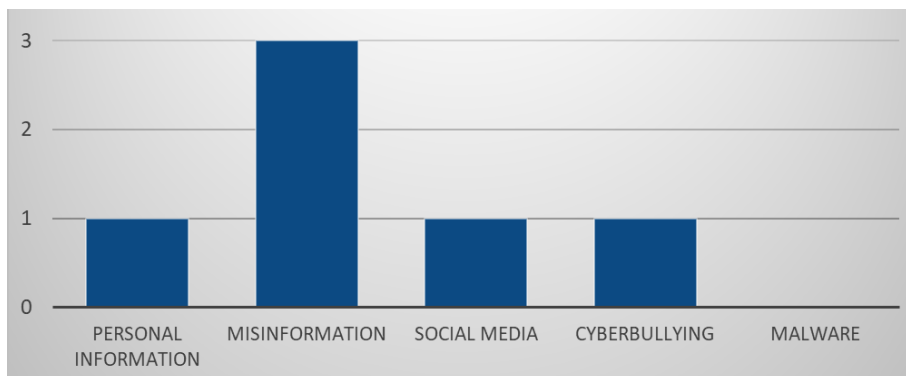
Teachers also gave many suggestions regarding activities. They mentioned that they have an **activity bank** that they can draw from for various lessons. We implemented aspects of this in some of our curriculums by having multiple different activities that teachers could choose from in their respective lessons. A teacher also mentioned a general **three part structure** he often followed: an introductory activity to get kids invested, an activity along with the lesson that delivers the content, and a final activity that cemented what the kids learned during that lesson. This helped us structure our own curriculum, albeit loosely.

Teachers recommended having activities that encourage **critical thinking** and involve having the students **discuss and write down their thoughts**. One example activity was making a word map; a concept would be written on a whiteboard at the center, and students would raise their hand and name what comes to mind. There were variations of this, such as simply listing topics as students brought them up, that we ended up implementing. Teachers also recommended using **scenarios** to teach lessons. For example, one teacher said that they would teach cyberbullying by having a student demonstrate cyberbullying by texting a teacher mean things, then having the class discuss what is going on, how it would make the student feel, how someone should respond, and how they would advise the teacher to address the cyberbullying. A different teacher recommended using real screenshots of scenarios online. We also got some suggestions regarding what activities wouldn't work. For example, for fourth graders, drawing activities wouldn't be as beneficial since they are capable of more complex thought to form ideas. This suggestion changed the concept for an early draft of the Social Media Safety & Mental Health module. Using the suggestions from our interviews with teachers, we were able to better shape our curriculum around the abilities of our students.

4.1.4 Digital Literacy 4 Parents Day Results

Besides teachers, another important stakeholder is parents. We got the opportunity to talk to some parents when Educall held an event called Digital Literacy 4 Parents, in which we were able to **hold informal conversations with parents**. This event occurred on Saturday, April 8th, and around 22 parents attended the event. Throughout the course of the day, we met six of these parents. From these conversations, we gauged that parents think all of the topics are important, but **Misinformation** is most pertinent to test first.

Figure 6: *Parents' Most Prioritized Topics*



Several governmental and other organizations also showed up to the event for presentations. We had a brief conversation with Simsim Participation Cityonne about their

Salam@ digital platform, translated by Vision School staff. Through this discussion, we learned about their work and about some information regarding passwords and login hacks, which was similar to the content we wanted to cover in our Personal Information module. We also learned about the other two organizations, E-Himaya and Academia Raquya, who are both part of the movement fueled by the Digital Development Agency (ADD). We learned how their platforms utilize aspects such as online quizzes and a mascot to help teach children. This additionally informed our curriculum.

By learning the desires of two of our most important stakeholders, parents and teachers, we were able to establish the most important digital literacy needs and begin to design our curriculum.

4.2 Digital Literacy Curriculum

Once we determined the major internet threats we should focus on, we could begin to design the curriculum around them. We wanted to follow Educall's lead in making education interactive and fun, and our activities represent that goal. Our curriculum contains five modules, each loosely following a **6 step structure**: Goal & Objectives, Time & Materials, Introduction, Activities, Assessment, and Conclusion. Each module should take between 2-3 hours, but they are left open-ended enough that teachers can add enough content to spread each module across several weeks. The modules are meant for a traditional classroom setting, but they have been modified to fit a fully online class as well. The material in the modules are appropriate for students anywhere from 9-17 years old with little adjustment.

The five major areas of focus that we identified are:

1. Misinformation,
2. Personal Information
3. Social Media & Mental Health
4. Cyberbullying
5. Malware

Because of this, we designed our curriculum to have five modules, each intended to teach about one of these five topics. Each module loosely follows a 6 step structure:

1. Goal & Objectives
2. Time & Materials
3. Introduction
4. Activities
5. Assessment
6. Conclusion.

The **Goal & Objectives** section tells educators about what the module is trying to teach and the major learning outcomes expected from students. The **Time & Materials** section tells educators how long the module should last assuming it is being completed in 1 session, as well as giving all of the materials and resources required to teach the module as written. The **Introduction** section asks students about their past experiences with the threats and how they dealt with them. It also introduces the major concepts and terminology in the module. The **Activities** section looks different for every module because activities will be more effective for some topics than for others, and each module is intended to feel unique so few activities are repeated. This section includes how all of the material is taught and reinforced, and provides teachers with activities and slideshows that can be used to teach the material to students. The **Assessment** section is also unique to each module, sometimes consisting of gamified online quizzes and sometimes of complex scenarios to be discussed in small groups and shared with the class. The ultimate goal of this section is to allow educators to see what students have learned from the module and to correct any misconceptions or incorrect thoughts the students might have taken away from the module. The final section in each module is the **Conclusion**, in which the educator summarizes the major takeaways from the module, asks students what they learned or how their behavior will change in the future, and addresses any final questions or comments. Using this model of module sectioning seems standard across curriculums of many different topics and fits our curriculum as well.

This curriculum is also built in a **relatively loose** way, providing teachers with some activities and resources to teach the content, but not holding them to the provided structure. Because the educator using the curriculum knows their students the best, it is built to be easily modified to better fit the students. Each module is meant to provide between 2 and 3 hours of content in a single session, but it gives teachers the ability to easily add or remove some of the content to better fit a time limit, or even to stretch the given materials across multiple sessions over multiple weeks if desired. Giving educators this amount of freedom was important to us when designing the curriculum because not all classroom environments are the same and it is important to adapt any lesson to their needs.

This curriculum was originally built to be taught to the 4th graders at Vision School, and as such the material should be appropriate for children 9 years and older. However, because of our opportunity to work with students from DigiGirlz as well, the material was slightly modified to suit the high school age group and converted into an online format. This makes the curriculum appropriate for students **anywhere from 9-17 years old**. It can be taught in both physical and virtual classroom environments for maximum versatility.

4.2.1 The Activities in Each Module

In building the curriculum, we wanted to make sure we were following Educall’s ideals for making education fun and interactive. We observed two of Educall’s classes, one of 4th graders and one of 2nd graders. We noted that the 4th graders were very enthusiastic and how the classes involved lots of participation, in particular a “word bubble”. We also noted the differences between the grades. This distinction helped us determine that activities **requiring students to raise hands** and offer suggestions would be good to include as there seemed to be no problems with getting them to participate. We aimed to use the students’ enthusiasm for participating to make our lessons engaging throughout, so it was very important for us to pair up each topic or objective with the best interactive activity. The results of these pairings are shown below in Figure 7, Figure 8, Figure 9, Figure 10, and Figure 11.

Figure 7: *Activities in the Misinformation Lesson*

Activity	Objective
Look at different examples of social media posts/news articles	To allow students to be able to identify the key aspects of verifying a source and being able to use critical thinking skills to explain
Bicycle Articles + Venn Diagram	To allow students to be able to identify the similarities + differences between the articles and being able to identify key facts
Competitive Online Quiz	To test student’s knowledge in a competitive and engaging environment

Figure 8: *Activities in the Personal Information Lesson*

Activity	Objective
Misinformation Tester	To see if the students can point out any red flags in the website https://Zapatopi.net/treeoctopus that may hint at it actually being fake
Personal Information Vocab	To test students’ knowledge on what personal information terms are and their importance personal information vocabulary terms
Digital Footprint & VPN Engagement	To engage the students and get them talking to each other about what they already know about digital footprints and what VPNs are
Pwned Activity	Get the students to go to the website https://haveibeenpwned.com and check if their or a parent’s email has been pwned

10 Minute Mail Maker	Have the students go to the site https://10minutemail.com and make a temporary email account and check it to protect future email accounts from repetitive verification codes
Surfing Safely	Have the students review 4 different websites and determine not only their validity amongst themselves but also what information they can and cannot give out to the sites

Figure 9: *Activities in the Social Media Safety & Mental Health Lesson*

Activity	Objective
Have students find the location where an image was taken using EXIF data	To get students to be aware that photos and other information students put on social media can contain a lot of personal information
Given a scenario on social media, write down how the student would respond on a worksheet and why in small groups	To help students understand social media safety and real situations one might encounter
Given a scenario regarding mental health on social media, have students discuss and raise their hands to suggest what to do	To help students think critically about situations that could impact their mental health online and prepare them for such situations

Figure 10: *Activities in the Cyberbullying Lesson*

Activity	Objective
Initial Discussions of Experiences with Bullying	To show students that cyberbullying is a real problem and get them to be sensitive to it
Showing a Short Cyberbullying Story	To further show the impact cyberbullying can have if it gets too far
Discuss Scenarios in Small Groups	To have students use their understanding of best practices for addressing cyberbullying and apply them to short scenarios

Figure 11: *Activities in the Malware Lesson*

Activity	Objective
Interactive Presentation	To get students accustomed to the vocabulary and teach the content in an interactive and engaging way
Matching Function of Types of Malware to Name	To solidify the names and functions in the students' minds
Ethical Hacking Group Activity	Brainstorm how the types of malware work together to accomplish the tasks; To ask the students to apply several of the concepts to a complex problem
Competitive Online Quiz	To test student's knowledge in a competitive and engaging environment

Using the list of activities we brainstormed, shown in section 3.2.2, and others derived through interviews and improvement, we were able to pair our learning objectives with effective activities. The results of these pairings were shown to Educall's staff and to teachers, and all claimed that the activities were well thought out, interesting, and useful in the classroom. After the first drafts of the lesson plans and activities were written, it was possible to test them in the classroom through our pilot programs.

4.3 Evaluation of the Digital Literacy Curriculum

We determined that the best way to evaluate the curriculum was through testing it in pilot programs. We ran a **pilot program for all five modules**, with one pilot occurring at Vision School with their 3rd and 4th graders as participants, and the rest occurring virtually using high schoolers and college students involved in DigiGirlz. We aimed to evaluate how each module felt from the educator perspective, and we asked students in a short survey how they felt about each session. Overall, the feedback was **very positive**, with students replying that they really enjoyed the lessons and feel like they learned a lot. However, the formal assessments built into some of the modules were not as productive as hoped, with **too few students** participating in either the pre- or post-evaluations to derive any concrete evidence of educational effectiveness. Because of this, our major recommendations for improving the curriculum include **instituting formal evaluations** into each of the modules and developing a better method to encourage students to participate in the evaluations. Other recommendations include giving more time to all of the modules than were provided in the pilot programs, as well as adding additional content to the modules that students suggested they were interested in.

4.3.1 The First Pilot - Misinformation

The first pilot program was run on April 12, 2023 using the **Misinformation** module, teaching both 3rd and 4th grade participants at the Vision School. Each class was held with about 15 students. The lesson was taught by Kavya Mani for both sessions, with Educall’s teacher Mohamed Benhsain overseeing, and each session was 45 minutes.

4.3.1.1 Misinformation Pilot - 3rd Grade

The third grade class was taught first. We first prepared all of the laptops that the students were going to be using by pulling up the first testable draft of the pre-evaluation, then handed out each laptop. We faced some technical difficulties since each google account was only able to submit one response and every laptop was using the same school account. To resolve this, we opened the pre-evaluation in an incognito window in order for students to reply without any overlap. The pre-evaluation took the entire length of the class since many students **did not understand the questions**, most notably the question asking about which news sources give the most accurate information and the questions involving a numerical scale rating their opinion from 1, “Strongly Disagree”, to 5, “Strongly Agree” (an example is shown below in Figure 12). We immediately began discussing how to improve the evaluations, and decided that the best course of action was to **simplify the language** in the questions and to change the numerical scale questions into multiple choice, with each answer being accompanied by words describing their comprehension (an example is shown below in Figure 13).

Figure 12: *Example Numerical Scale Question*

Do you agree that you can permanently remove something posted on the internet?

	1	2	3	4	5	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

Note. Above displays an example of a numerical scale question that we had in our evaluation. Students were intended to select a higher number for more agreement or understanding of the topic, but our collected data and our experience working with the children in their class showed us that they did not understand what the question was asking.

Figure 13: *Example Multiple Choice Question*

How good are you at using technology?

- Very good
- Good
- Okay
- Bad
- Very bad

Note. Above displays an example of a multiple choice question that we had in our evaluation to ask about students' understanding of the topic. We hoped that by assigning adjectives to each choice it would be easier for children to understand how to answer the questions.

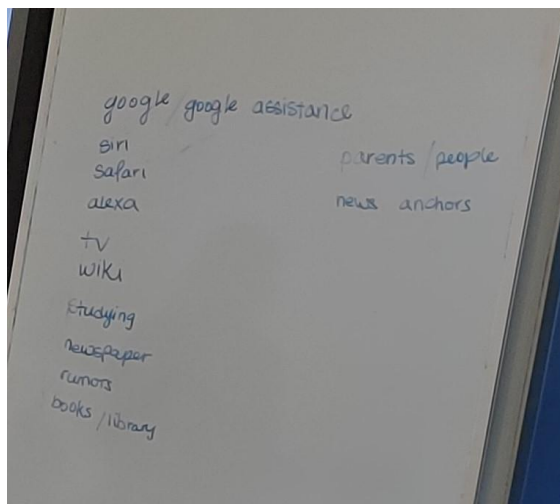
4.3.1.2 Misinformation Pilot - 4th Grade

The second lesson was taught to the 4th graders. The class was delayed 10 minutes due to the students arriving late and needing time to get settled. Because of how long it took to get through the pre-evaluation with the 3rd graders and our short time with the class, we decided to **skip the evaluation** in favor of immediately starting the lesson. Kavya began the class by asking

the class to brainstorm where they get their news and information. All the students were very **eager to answer**, giving answers including books, football news channels, family members, and other sources, which was written on the whiteboard shown below in Figure 14. Then, she moved to the slide showing other examples of sources. This process took about 15 minutes, which was a lot longer than we expected. Next, she asked if they knew what misinformation is, which they responded affirmatively to, providing their own definitions and examples when asked. She then discussed the difference between misinformation, disinformation, and malinformation. The students appeared to be following the instruction, but they were still excited from the earlier interactive sections and may not have been as focused on the material. Then, the three different examples of misinformation were shown, including a headline about a man using a flamethrower to clear the snow, a social media post about the CEO of Facebook coining the term BFF and encouraging users to comment it across the entire site, and another social media post about needing to share that post or risk being charged for using their account. For each of the scenarios, all of the students used their critical thinking skills to **determine whether the scenario is misinformation** by examining the posts and pictures. The session ended with Kavya showing the last slide regarding ways to verify a resource, including by examining the author, the date the resource was written, whether it was published in a reputable source, and the author's intent for the resource. She also gave the 4th graders some homework to research the definition of bias. At this point, the session was over and the students had to move to their next class, so we were **not able to use our evaluation activity** to test whether they internalized the material.

Figure 14 : *List of Sources of News and Information that Students Answered*

- Google assistance
- Siri
- Safari
- Alexa
- Tv
- Wiki
- Etudying
- Newspaper
- Rumors
- books/ library
- parents/ people
- news anchors



4.3.1.3 Misinformation Pilot Feedback and Recommendations

After running the pilot, we met with the supervising teacher, Mohamed, to evaluate how the pilot went. He offered suggestions for what we should change for the next pilot, including that **3rd graders have less mature vocabulary** than 4th graders, so some of the questions on the evaluation may be too complex for them. Going forward, we decided that we should **simplify** the evaluations we made, and we **translated them to French** for the 3rd graders. He also mentioned that the session with the 4th graders went better, with this particular group of 4th graders being generally very curious and talkative.

Mohamed also advised that as we only have 45 minutes for the pilot, we should prepare around 30 minutes (70% of the time) for content and leave 15 minutes for questions or interaction with the students. We took this advice and changed the expected times of the activities and of the entire lesson for all five of the modules for better usage in the classroom. He also advised that when teaching, it was best to only take 5 questions for each powerpoint slide in order to better manage the short time that we have to teach, which was useful moving forward with further pilots.

4.3.2 The Second Pilot - Social Media Safety & Mental Health

The **Social Media and Mental Health** pilot was run by Kaley Du, with Kavya Mani taking notes. This pilot was run virtually on Google Meet with DigiGirlyz. Kavya also assisted with finding and pasting links for evaluations, which was a method of teamwork we found would be effective to use in the future. The pilot consisted of about a total of 44 students; some students went back and forth between different breakout rooms throughout the session, but 20 students were consistently in the lesson at all times.

4.3.2.1 Social Media Pilot Pre-Evaluation Findings

The lesson started with giving students a pre-evaluation to assess their current level of knowledge by posting the link to a Google Form in the chat. This testing took about 10-20 minutes. There were some technical difficulties in getting the link in the chat, as Kaley had some trouble getting the link and the wrong link was posted at first. However, we were able to collect a strong sample of **20 responses** in the pre-evaluation about social media safety and mental health.

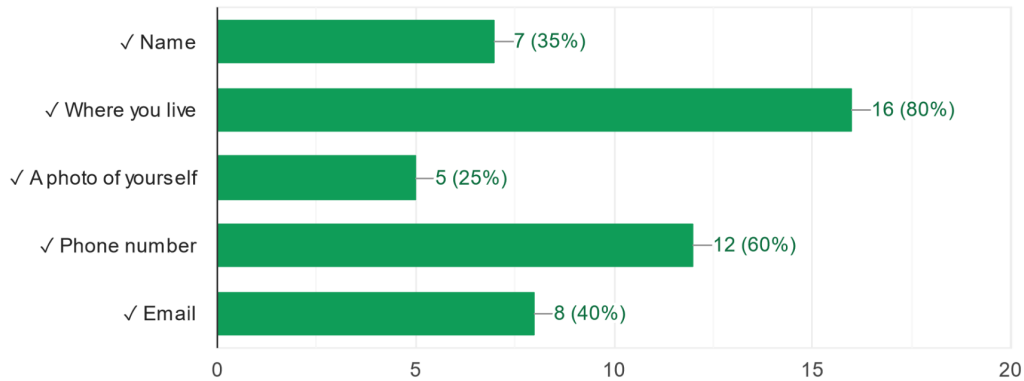
One question in the pre-evaluation that had zero correct responses was a multiple selection question about what information they should avoid posting on social media publicly. The answers that students selected the least included a photo of themselves, their name, and their email. A larger percentage of students answered “phone number” and “address”, 60% and 80% respectively. As only three respondents only checked one answer, confusion regarding the multiple selection format likely did not skew the results much; however, an extra reminder to “select one or more” of the answer options may help. This shows that the students have some

knowledge about information they shouldn't post on the internet, but some blindspots regarding other information.

Figure 15: *Responses To Pre-Evaluation Question “What Information Should You Avoid Posting on Social Media Publicly?”*

What information should you avoid posting on social media publicly?

0 / 20 correct responses

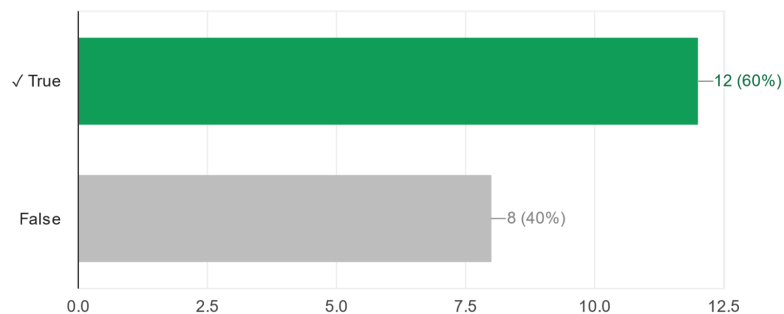


Another question that had a high incorrect response rate was: “True or false: you should never meet up with a person you met online”. 40% of respondents answered false, which was the incorrect answer. This showed a special divide in this regard.

Figure 16: *Responses To Pre-Evaluation Question “True or False: You Should Never Meet Up with a Person You Met Online”*

True or false: you should never meet up with a person you met online

12 / 20 correct responses



4.3.2.2 Lesson on Social Media Safety & Mental Health

Kaley first began the Social Media Safety & Mental Health presentation by introducing the topic. She posed a prompt to have students raise their hand if they used social media, and then had them type what social media platforms they use in the chat. The students gave responses such as **YouTube, Tiktok, Instagram, Discord, Pinterest, Facebook and WhatsApp**. Then, she moved on to discussing what information not to share on social media. Students typed answers in the chat, and some raised their hands and unmuted to give their answers. In the chat, many people answered addresses, anything that could reveal where they live, name, and passwords. There were some **answers that contested each other**, including whether it is safe to share one's age on the internet, since it may make a minor a target to adults with malicious intent, but it will also allow a student to be aware if someone is the same age as them. This resulted in some good discussion. Kaley affirmed that it is generally a bad idea to share age on the internet. One possible addition to this discussion could be that one can mention that they're a minor but not mention their age specifically.

Then, Kaley went over a slide about **image metadata** and the information others can learn through an image on social media. She skipped a video for time constraint reasons, but discussed that photos have metadata that can include location, that some forums don't scrub metadata, and that geotagging on phones can record a person's location. She then gave an example of how once, on the internet, people found where someone worked by looking at an image that that person posted's metadata. She also mentioned how a reverse image search, reflections in glasses, windows or screens, and possible landmarks can reveal where a photo was taken. She didn't ask any questions about this slide since she wanted to just cover it briefly.

Next, Kaley showed an **example of some messages** students might encounter on social media. The first message was of a direct message from a random stranger. Students were once again asked to raise their hands and respond. A few students answered that they would **block** the stranger or simply ignore them. One answered that they might respond just to **figure out who** the messenger is, since the stranger can not gain any information about the student if the student does not give them any personal information, and then block them after. Kaley then affirmed the answer of blocking the stranger being the most preferred option. She also mentioned that some messages can be a random stranger trying to be flirty or calling someone beautiful, which is a situation where they should definitely block the stranger. However, she did give a slight bit of leeway, stating that if one messages the stranger, they should be very careful.

The second example involved a person with whom the student had already been chatting, but began mentioning that they should meet up and became a bit pushy when the student hesitated. The students' responses included that they should not because it's a **bad idea in general to meet up** with a stranger on the internet, and because they seem manipulative with how pushy they are. There were also suggestions about **telling a trusted adult** about this person. One student said that if they'd been talking to the person for a long time and had built up trust and a bond that they could possibly meet with them at a **public place** and while **bringing another person**. Another student countered that even if they built up some trust they **still wouldn't meet the person**. Some also responded that they should **block or ghost** the person. A

different student responded that they would meet the person, but they would tell a friend or person they know what they're doing and go to a public place. Kaley's "official" answer was that in this situation, since they were being pushy, it would be best to not meet them and possibly block them. She also mentioned the student should tell a trusted adult, and that if they really felt in danger they could tell the authorities. However, she discussed that if a student had to meet up with someone, it would be when the student is an adult, and along with the suggestions given earlier, they should tell someone where they're going, meet at a public place, and go with someone else. This **may have caused a bit of confusion** because one question in the pre and post assessment was "True or false: you should never meet up with a person you met online", with the correct answer being false. It is probably better when teaching to err on the side of caution and tell students not to meet with strangers on the internet. However, there are some reservations about it being entirely impossible to do so. Going forwards, we may change the wording on this question.

Next, Kaley went on to a slide about predator tactics. She asked the students if they heard any stories about predators online. Students responded that they've **heard lots of situations**. One student mentioned how women, especially young women, **are seen as targets online** since they're viewed as a more naive and vulnerable population; in addition, predators will often **feed a victim affection**, using phrases such as "you're so mature for your age". Another student said how predators will gain one's trust, and then get the student to send them photos that one wouldn't want leaked publicly, using these as leverage and **blackmail** to get them to send more and trap them in a cycle. They mentioned that the law is on the side of these victims, and they can report these predators, but many people **don't know about the law**. She also mentioned how there might be an **atmosphere of shame surrounding** the victim, which is a reason why they might not tell anyone about it. Another student brought up a point about how predators are becoming more creative with their methods, and that they will try to get their victims to **emotionally rely** on them and keep them coming back to them. These predators will seek out those with low self-esteem and get the victim to latch on to them. One student also mentioned how some predators will try to hack people and threaten them to do certain things in order to get what the predator stole back. Kaley then read out the predator tactics she had on the slide, trying to point out more specific techniques such as flattering people, isolating them from friends and family, and possibly impersonating someone they know. A lot of what she wanted to mention **was covered by the discussion**, which was a good indicator; however, it also showed that she **underestimated** what the DigiGirlz students would know.

She then mentioned a specific example from a news article that happened with a 13 year old Singaporean who was talking to an adult from the UK. She pointed out how the predator tried to gain her trust at first by being nice and saying that the victim could always rely on her, and that later on it escalated to the predator trying to find where she lived.

The next example was a scenario in which a friend invited a student to a group chat, and when someone posted something inappropriate in the chat, no one reacted to it. Most responses stated that the student should **leave and report** the chat. Some also mentioned they'd warn their

friend and tell a trusted adult about it. Kaley said the “correct” answer was the same as their responses. She then went on to note the risks of group chats and forums, and how there could be a lot of toxicity in the bad circles. There was another student that mentioned that they never really use forums because of the possible toxicity and that they’d rather interact with real people. Another student **countered that there can be lots of positive experiences** with finding like minded people in group chats or forums, such as with fandoms, and that as long as there are responsible moderators and rules are followed that there can be good experiences. Kaley affirmed this, trying to get across that there are many possible positive experiences with online communities, but it’s important to be aware of the dangers. She also mentioned how there could be moderators who aren’t responsible, and used a worst case example of mental health forums that actively encourage people to get worse.

Finally, the last discussion question was asking who a person could go to if sent inappropriate content. The students mostly said a **trusted adult**, and also added that they should **block and report** the person in question. One student also mentioned that parents can be strict, so someone might not want to tell them about a case like this; in that case, it may be better to mention it to a teacher or another trusted adult. The next slide indicated they should block and report, tell a trusted adult, generally don’t get involved, and even report to the authorities if the student feels unsafe.

Kaley ended with a slide about having a conversation about the internet with parents and others. Then, she posted the post-evaluation with the questions she didn’t cover taken out, and Kavya posted the survey about how the students felt about the pilot.

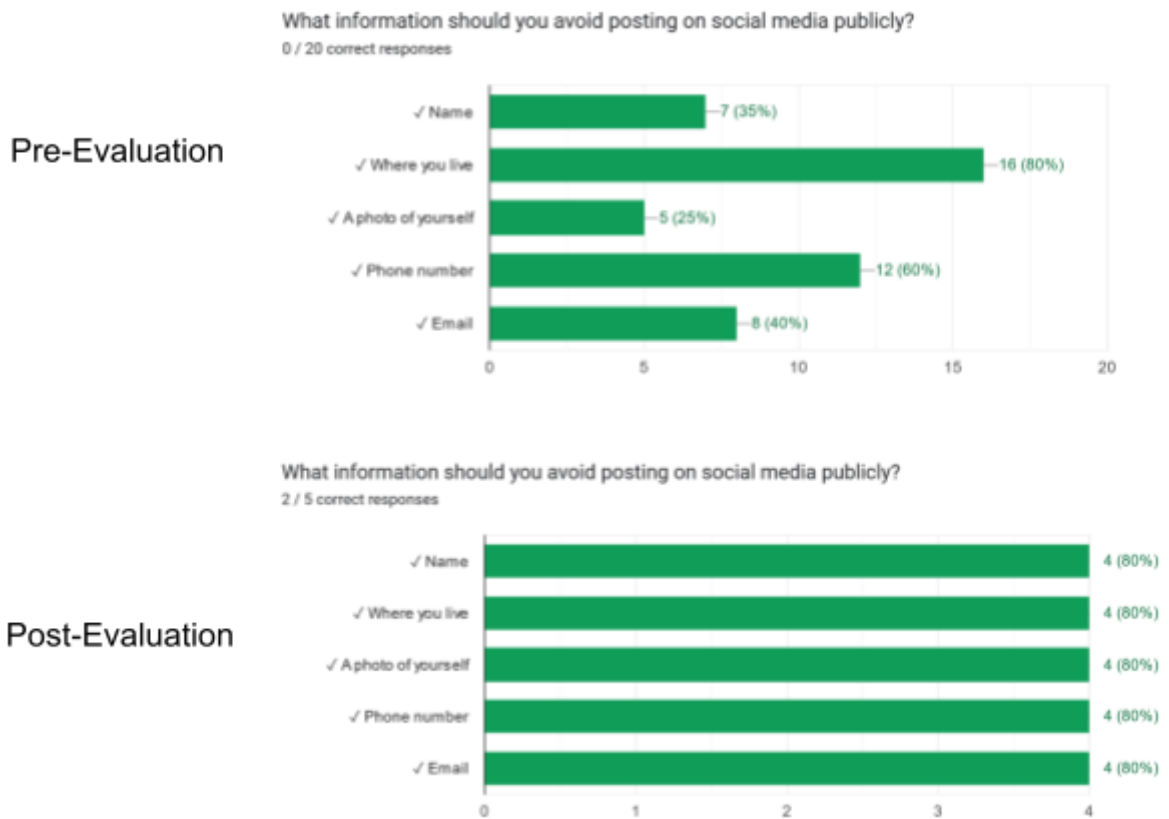
Overall, Kaley found that she may have **underestimated the amount of knowledge** the students had. As the curriculum was originally designed for 4th graders, witnessing the pilot session with that age group gave a skewed perception of what the high schoolers might know. At first, she was even doubtful that the DigiGirlz students had heard about what an internet predator is, how to block and report, or what photoshop is. The students often pointed out answers during discussion to the content Kaley was aiming to discuss beforehand. As the pilot progressed, there also seemed to be less responses, which could indicate a lowering interest; however, it may just be that the final question was more basic. These results allow us to adjust our Social Media Safety & Mental Health module based on this new baseline we have acquired.

4.3.2.3 Social Media Pilot Post-Evaluations

A problem with the post-evaluation was that **there were only 5 responses**, while the pre-evaluation had 20. This made our collected data less useful. A recommendation regarding this issue is to have an extra reminder both at the beginning and end of the lesson to fill out the post-evaluation. In addition, the instructor could also have the pre and post evaluation links **displayed somewhere** throughout the entire session on an online session, or write them on a whiteboard in front of the class in an in person class.

Although the results for the post-evaluation were insufficient, they showed a general **increase in knowledge** of the content covered. For example, for the question regarding what information students should avoid posting on social media publicly, all respondents answered correctly, shown in Figure 17, as compared to the zero respondents who answered correctly in the pre-evaluation.

Figure 17 : *Pre-vs Post Survey Responses to the Multiple Selection Question “What Information Should You Avoid Posting Publicly?”*



As another example, the question in Figure 18 shows that, in the pre-evaluation, some students gave the incorrect answer of “You can reveal some personal information to those who seem trustworthy”, but in the post-evaluation no student answered incorrectly. In addition, for the question of whether a student should meet someone online in person, as shown in Figure 18, in the pre-evaluation the ratio of students that answered correctly was 60%, while the ratio of students in the post-evaluation that answered correctly was 80%.

Figure 18: *Pre-vs Post Survey Responses to the Multiple Choice Question “What is a Rule You Should Follow in a Public Group Chat?”*

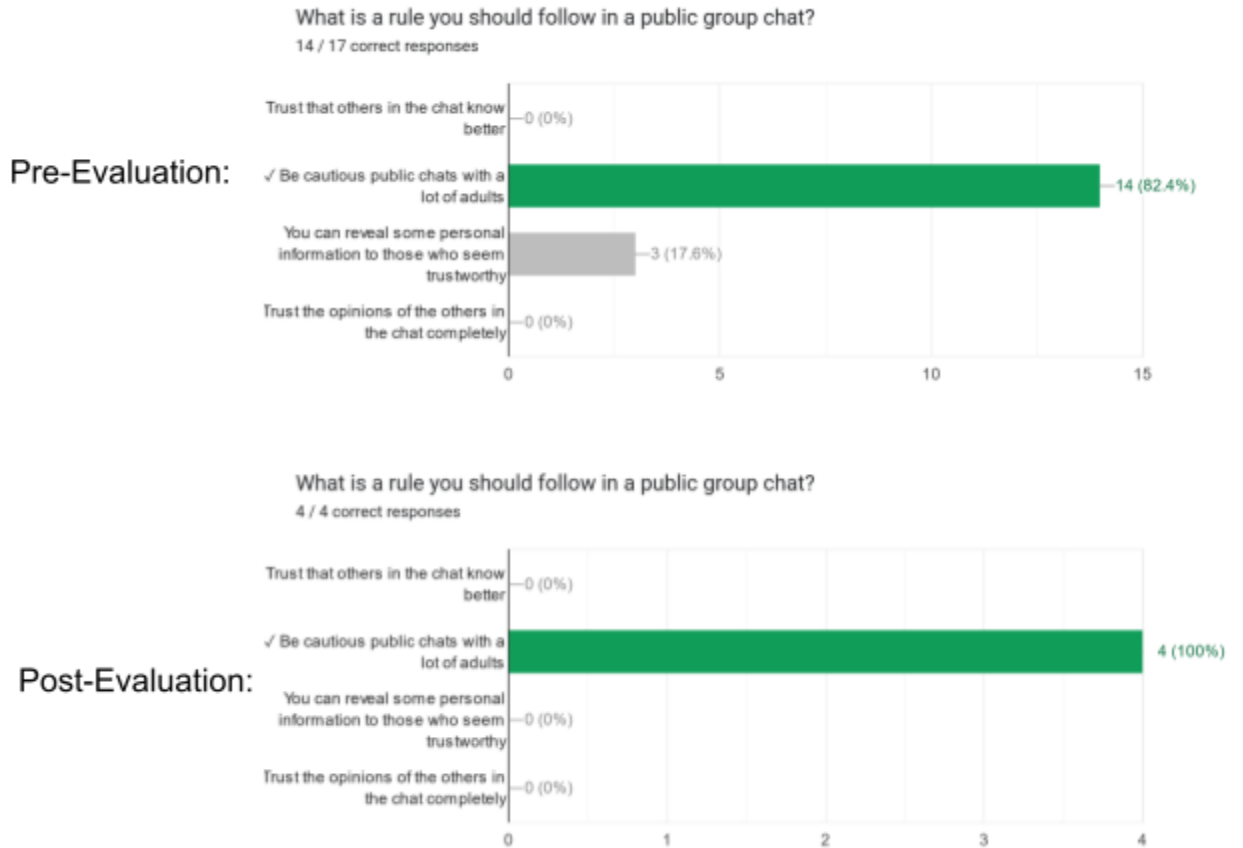


Figure 19: *Pre-vs Post Evaluation Responses to the Multiple Choice Question “True or False: You Should Never Meet Up With a Person You Met Online.”*



The post-session satisfaction evaluation also produced some relatively good results, with an average rating of **3.78 out of 4 for enjoyment** and **3.33 out of 4 for the amount students felt they learned**. Some significant suggestions were for there to be greater discussion of personal experiences. There were also some students who were confused about some parts of dealing with strangers on the internet, such as whether or not to respond to them in direct messages or whether they can safely meet a stranger in person. While the standard answer to both of these questions is that they shouldn't, there could be room for a bit of interpretation in specific instances where these would be okay. It would be best to lay these out as rules, but also allow debate between students.

4.3.2.4 Recommendations for the Social Media Module

A goal for the next run through of this session with a high school aged group would be primarily to make some of the **questions more complex** and allow for more **sharing of personal experiences** and in-depth discussion. For example, the instructor could ask more questions about what the consequences are for revealing certain pieces of information on the internet, and follow the presentation with a free discussion on their own experiences on the internet and what they will change from now on. In addition, **more time** must be made for this module, and it will need to take multiple sessions in order to cover all the material. Our team would recommend running the part of the curriculum related to social media safety as one session, and the parts about

netiquette and mental health as another session. However, even these two halves may take more than one session depending on the time allotted and how in detail the instructor wishes to go.

4.3.3 The Third Pilot - Malware

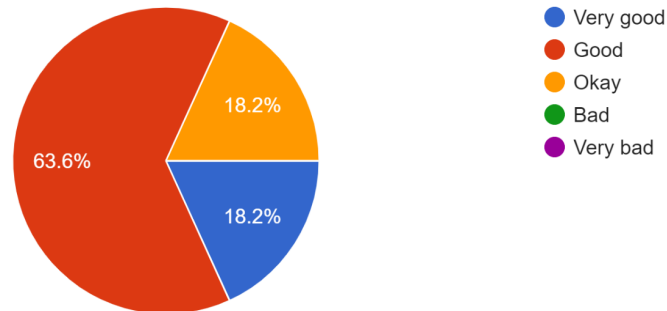
The pilot of the **Malware** module was run online (Google Meet) with DigiGirlz, with Patrick Bailey teaching and Ethan Reed taking notes and offering support occasionally. This lesson had an average of **25 attendees**, with attendees being able to switch between this lesson and the Social Media & Mental Health lesson discussed above. It was taught over 1.5 hours. This lesson began with Patrick introducing himself and Ethan, including that they came from the United States and were working with Educall to develop a digital literacy curriculum for Moroccan students. This lesson included an interactive slideshow presentation that asked students to think about what malware looks like and the best ways to avoid it, as well as short scenarios asking students to examine what malware-related events look like, diagnose what was happening, and react appropriately. This presentation was concluded with a short online quiz with gameplay elements such as points, encouraging competition. This lesson went very well, with student feedback being very **positive**. The major recommendations for this module include **more time and additional activities** to solidify vocabulary in the students' minds, including additional content about cybersecurity and the field of ethical hacking as per student suggestions, and producing questions that better gauge how much students learned from the module.

4.3.3.1 Malware Pre-Evaluation Findings

Patrick first began the lesson by introducing both himself and Ethan, that he came from the United States, and that he was working with Educall to develop the digital literacy curriculum, which would be taught now. He first asked students to fill out a pre-evaluation regarding their demographics and their background with the topic, which was constructed in Google Forms and distributed through the Google Meets Chat function. **11 participants** responded to this pre-evaluation. We found that the respondents in this lesson came from high schools and universities all across Morocco, with ages ranging from 14-18 years old. All respondents used cell phones, 9 used computers, 4 used tablets, and 2 used school computers, with all of them using technology every day. As seen below in Figure 20, respondents felt **generally competent** at using technology, with none of them thinking their abilities were “Bad” or “Very Bad”.

Figure 20: *Malware Pilot Participants Evaluate Their Technology Competence*

How good are you at using technology?
11 responses



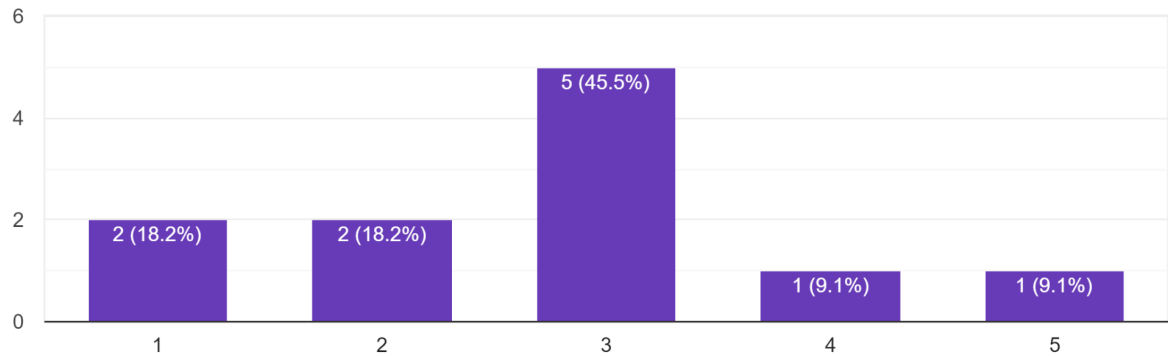
Note. These are the results of the question posed in the pre-evaluation for the Malware lesson. None of the respondents said they were bad at using technology, while most thought they were “Good”.

This pre-evaluation also asked students how familiar they were with the concepts of malware and computer viruses, as well as how skilled they are in avoiding downloading computer viruses. These results are shown below in Figure 21 and Figure 22.

Figure 21: *Malware Pilot Participants’ Familiarity with Malware and Computer Viruses*

How familiar are you familiar with the concept of malware and computer viruses?

11 responses

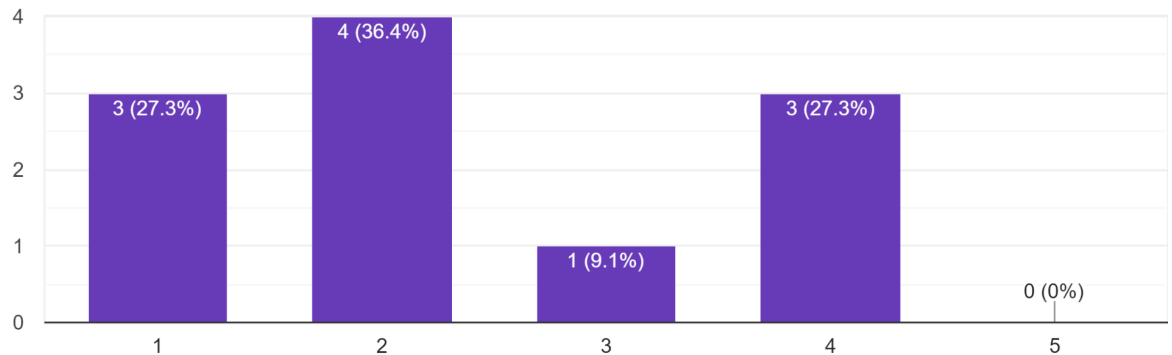


Note. These are the results of the question posed in the pre-evaluation for the Malware lesson. Most of the respondents felt slightly familiar with these ideas, with many feeling very unfamiliar with them.

Figure 22: *Malware Pilot Participants' Skill in Avoiding Downloading Viruses*

How comfortable are you in avoiding downloading viruses?

11 responses



Note. These are the results of the question posed in the pre-evaluation for the Malware lesson. Most of the respondents felt like they were uncomfortable in avoiding downloading computer viruses.

Additionally, **54.5% of these respondents used antivirus** software, while 36.4% did not, with 9.1% having never heard of antivirus software before. Despite this, 63.6% ranked the importance of antivirus software as a 5 on a scale from 1-5, with 9.1% putting it at a 4, and

18.2% at a 3. The respondents also said that they **protected their privacy in various ways**, including some replying that they used antivirus software, some replying that they used VPNs or other location-protecting software, some saying they avoided suspicious websites, and some saying they did nothing.

All of this indicates that the topics and vocabulary covered in this lesson will be **understood by students** at this age level, with them having some starting knowledge about the topics but still being in need of further teaching for expansion of their skills in addressing and avoiding these threats. Because it is unclear whether younger students can understand these topics, **additional surveying** should be done with younger students to determine the extent of their knowledge about malware, and this should be used to tailor the lesson for them.

4.3.3.2 The Malware Lesson

After the evaluation was posted and students were asked to complete it, Patrick began the introduction to the lesson. He first asked the students how they would define malware and whether they had any past experiences with it. Students unanimously responded that they were **somewhat familiar** with malware, and one of them provided an example of a scareware message claiming that they had downloaded a trojan virus. However, they said that they were not sure what that really meant, and they dealt with the message by simply closing it. Patrick was then able to begin the lesson with the students' starting knowledge in mind.

Patrick began to move through the slideshow presentation, trying to encourage participation and constantly checking the chat for questions. The presentation was built to be interactive for the students, including a short activity **asking students to guess the function** of each type of malware. Since the initial slide introducing each type of malware contains pictures detailing the function of the malware, Patrick was able to ask students what they thought the type of malware might do. He then went through the definition and function of the malware and told the students why and how the malware causes problems. After these slides, the class arrived at the "What can you do if you get malware?" slide, which allowed the students to share about how they thought malware should be addressed. The students seemed to **already have the right idea** about how to deal with these types of problems, but they were not fully correct and Patrick was able to add to their ideas. Then, Patrick moved through the antivirus slides, talking about the numerous abilities and benefits of using antivirus software, before beginning the "How to get malware" slides. These slides are very similar to the "Types of malware" slides, and Patrick was able to encourage the same type of student interaction. Patrick was also able to ask students about whether they had ever needed to deal with these types of threats, and allowed students to share their experiences that way as well. This was especially true in the section about phishing, as it is the most common threat and almost all the students had seen phishing emails or messages in the past. There were **many good questions** Patrick and Ethan were able to answer during this section, which showed the students were following the lesson but were interested in learning

more about these topics. Overall, Patrick was able to encourage a lot of student participation during this lesson, including allowing students to ask questions that showed that they were understanding the topics covered and wanted to learn more, which can be viewed as **successes for the presentation format** used.

The next activity of the module asks students to take the concepts that they just learned and apply them to **open-ended scenarios**. This activity was intended to be given to the class after it was divided into small groups, but due to limitations in the online format, the scenarios were instead placed at the end of the slideshow to be discussed as a full class. The first scenario asked students to recognize the symptoms of a successful phishing attempt and describe how malware could be used to break into a person's social media account. The students quickly decided the scenario was the result of a successful phishing attempt, but **struggled in determining what types of malware** could be used to gain unauthorized access to a social media account. The next scenario asked students to recognize a successful malvertising attack that installed progressively worsening adware on the system. Students were able to diagnose that the attack was caused by adware, but were not able to name the fact that malvertising was involved. The final scenario asked students to brainstorm some ways a hacker could earn money by installing malware on their systems. The class was able to answer this question as a large group, with several students **each contributing one method** of earning money. Overall, this activity seemed to work pretty well, with students showing that they understood what was taught in the lesson and being able to **apply these concepts** to real-world-like scenarios. The students were very happy to participate, and they seemed to be **engaged** in the activity throughout its length. A recommendation to improve this activity is by **doing it in small groups**, as originally intended, to allow all students to share their thoughts and to build collaboratively with others. During the lesson, the same small group of students were the ones to answer most of the questions, so by doing the activity in person and in small groups, more students will hopefully be able to share their thoughts. Another recommendation for this activity would be giving it **more time**, as the 1.5 hours allocated for the whole lesson forced all sections to become faster and more compact. By giving more time to this activity, it will allow students to think more completely about the scenarios. Finally, it seemed like it would benefit the students if they had a **reference guide** to the types of malware discussed in the presentation. This would make it easier for them to use the full list of terms, rather than just what they remember, which will give them more ability to think about the extent of the scenarios.

The final activity of the module was an online quiz with gameplay elements like points that encouraged competition among the students. This section went well, and Patrick was able to see where students were confused after each question, explain why the correct answer is correct, and clarify things to the students who gave an incorrect answer. The students seemed to really enjoy this activity, and it can definitely be used as a sort of post-knowledge assessment to test the effectiveness of the lesson. However, it is recommended to modify the questions, as some questions were not explicitly covered in the lesson and some questions were confusing due to the wording of the question rather than due to the content covered. The format of this sort of

gamified quiz allows students to be more engaged due to its gameplay elements, and allows the educator to see what students thought at the end of every question, which have shown to be major strengths in this sort of lesson.

This session was concluded by summarizing the key takeaways of the module, asking students how they will keep themselves safe from malware, and encouraging students to stay safe online. Students were thanked for their participation, and they were asked for any final questions or comments, which were addressed. A short final feedback survey was distributed through the Google Meets chat, and students were asked to fill it out before they left.

4.3.3.3 Feedback and Final Recommendations for Malware Module

At the end of the Malware module pilot, a short, anonymous feedback survey was distributed to ask students how they thought the class went. This survey received **8 responses**. Respondents were first asked to rank their enjoyment of the lesson and how much they thought they learned on a scale from 1-4. Their average **enjoyment was calculated to be 3.75**, and the average rating for the **amount that they learned was calculated to be 3.50**, with the lowest rating for either category being a 3. These numbers can be taken to mean that students greatly enjoyed this lesson, and that they feel like they learned a lot, which means that the lesson was very successful. Respondents were next asked what they enjoyed about the lesson, whether anything was confusing, and whether they had any suggestions for other activities. 4 of the respondents specifically said that they really **enjoyed the online quiz**, and 4 said that they thought the **information was taught very well**. None of the respondents gave any negative criticism, although one respondent thought it would be useful to **spend more time with the vocabulary** and one other was interested to learn more about **how antiviruses work**. This can all be taken to mean that the students really enjoyed the lesson and that all of the ideas put into it work well.

There are some final recommendations that we hope anyone teaching this module in the future can use. Firstly, **giving this module 2.5-3 hours** to teach rather than just 1.5 would be very beneficial, as it felt like the educator was constantly rushing through the content. It would also be beneficial to allow students to spend more time with the vocabulary. Secondly, this module needs to undergo a **better test of effectiveness**, including pre and post tests, to verify that it can deliver its content well. The online quiz included in the lesson proved to be enjoyable for the students, and it gives the educator a good chance to redirect any misguided thinking the students display, but due to its competitive nature it may not be the best evaluation of the student's final knowledge. To effectively measure whether the module teaches well, a formal pre and post evaluation should be administered. The major recommendations for how this module should be changed include giving it more time so students can spend more time with the material and vocabulary, and to institute formal knowledge assessments to measure how effective the module is at teaching.

4.3.4 The Fourth Pilot - Cyberbullying

The cyberbullying pilot was run by both Patrick and Kavya. This pilot was run **virtually with DigiGirlz**, and it consisted of a total of **26 students**, with some students going back and forth between this session as well as the personal information session. However, there were consistently **about 16 students** throughout the entire cyberbullying pilot session.

4.3.4.1 Cyberbullying Lesson

The lesson was in a discussion format. It began with Patrick introducing the session and asking the participants to **describe what cyberbullying** was. One participant said it was “picking on someone online behind the screen and belittling them [...] and making them think that they are not enough and that no one is immune to [...] bad [comments]”. There were other comments that described cyberbullying as people posting unpleasant comments online that are hurtful to the victims. Then, Patrick asked participants to describe their experience with cyberbullying or any stories of cyberbullying that they have heard of, if they were comfortable enough to share. The general themes of the responses were: people commenting on the victim’s social media saying they are beautiful, then **circulating the victim’s pictures** through various groups while pointing out insecurities in the victim’s appearance or personality. The students commented that they have **not experienced severe cases** of cyberbullying and have only been to the extreme of teasing. Then Patrick asked how they could get out of a cyberbullying situation. There was a lot of participation: students stated that one should **report** targeted comments or **ignore** it so the bully does not get the attention or reaction that they want. Patrick also posted a link into the chat on how to prevent cyberbullying and explained exactly what needs to be done in a cyberbullying situation. Then, Kavya asked what influences a person to become a cyberbully. Responses stated that when a **person is insecure** and they lack some sort of control, they try to gain a sense of control by becoming a bully. Another answer was that a bully could be a victim of bullying and feel that becoming a bully is the only form of escape.

The lesson then moved towards **analyzing a short film** and being able to interpret various aspects in the video. The video was called “Are you okay?”, an Award-Winning Short Film by Fight Abuse Channel. The video was stopped at random yet significant break points to identify symbolism, what the main character is doing, and the foreshadowing and the meaning behind each segment. Students were consistently able to collaboratively understand the symbolism, and they had a **long, interesting discussion** as a class about each stopping point. They showed that they did understand all of the effects of cyberbullying in both symbolic and realistic portrayals, and they as a class really enjoyed the discussion we fostered. The class

continued watching the video for the rest of the allocated time. Overall, the lesson went very well, and it was a great space for students to discuss their experiences with cyberbullying.

4.3.4.2 Feedback and Recommendations for Cyberbullying Module

At the end of the cyberbullying session, an anonymous survey was given to all the participants for them to rate their enjoyment and how much they learned from the session and if there were any shortcomings they noticed or suggestions they wanted to make. There were **11 responses with all being very positive**, rating the satisfaction and amount learned during the lesson between 3-4 out of a scale of 4. The average **rating of their enjoyment** was calculated to be **3.82**, and the average rating of the **amount they learned was calculated to be 3.73**. In the student recommendation section, almost everyone responded that they really loved the **open discussion** and the topics discussed during the lesson. The feedback for this lesson was extremely positive, and it showed us that this module was designed very well for student enjoyment.

The only major recommendation that came out of this session was to **provide more time** for discussion; it was extremely productive, but not everyone was able to share their views due to the limited amount of time. By giving more time to the module, more scenarios will be able to be presented and students will be able to share more of their thoughts in the discussion.

4.3.5 The Fifth Pilot - Personal Information

The pilot of the Personal Information module was run by Ethan Reed and Kaley Du. This pilot was run virtually working with DigiGirlz as well. This pilot consisted of a total of **26 students**; some of whom switched back and forth between this personal information lesson and the cyberbullying lesson.

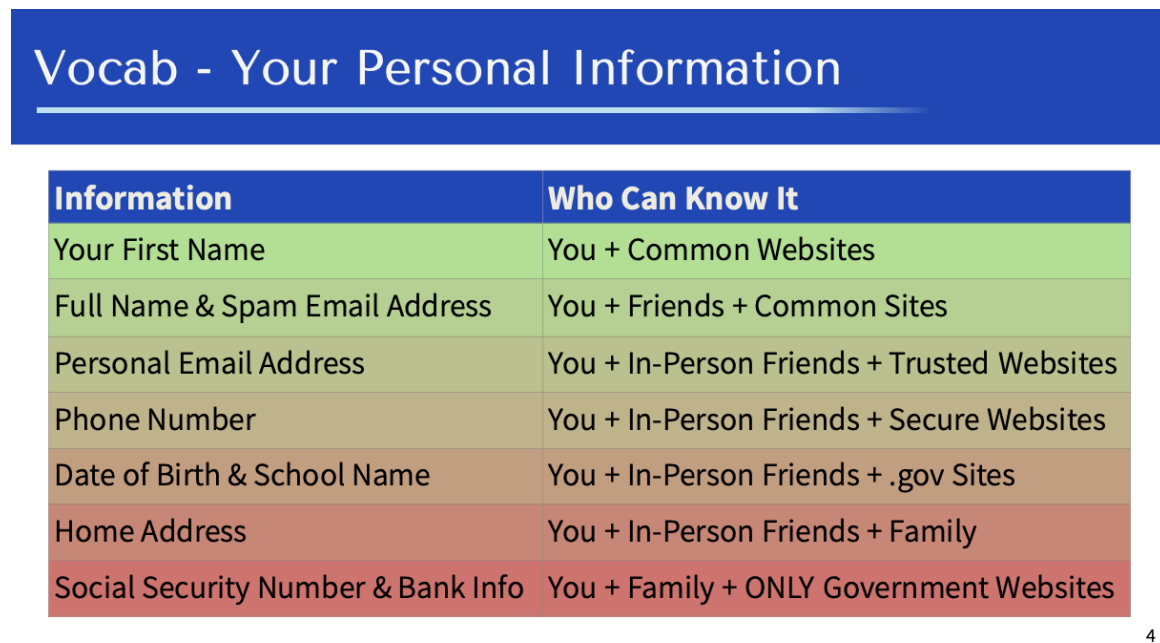
4.3.5.1 Personal Information Lesson

The Personal Information module aimed to deliver a discussion-based format while going through a slide deck. The pilot opened with a **misinformation exercise** where the students would go to a misinformational website and determine whether the information presented was legitimate. A student responded that it was factual information due to the lock symbol next to the url, but Ethan explained it was not legitimate, saying that the sources used were also all false and that, if examined closely, it was possible to tell they were unreliable.

The opening activity was followed by a slide that had a table discussing some **vocabulary**, such as some personal information terms along with who it can be shared with.

Ethan asked the students which of the terms they had heard before and what information other people on the internet may want from them. One student responded that they would want a **person's address**. After speaking with the students and going over numerous pieces of information that people try to steal, another slide, shown below in Figure 23, broke down all of the new terms that they just learned.

Figure 23: *Personal Info and Where You Should Share It Online*

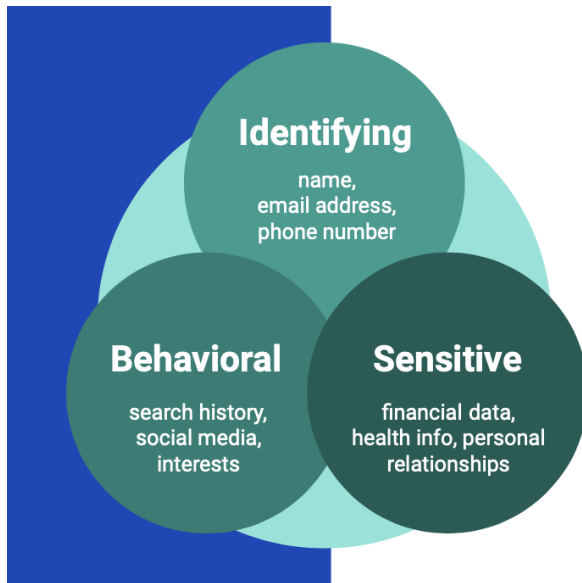


Information	Who Can Know It
Your First Name	You + Common Websites
Full Name & Spam Email Address	You + Friends + Common Sites
Personal Email Address	You + In-Person Friends + Trusted Websites
Phone Number	You + In-Person Friends + Secure Websites
Date of Birth & School Name	You + In-Person Friends + .gov Sites
Home Address	You + In-Person Friends + Family
Social Security Number & Bank Info	You + Family + ONLY Government Websites

4

These vocabulary activities were followed by Ethan breaking the vocabulary down for the students into three main categories: **Identifying, Behavioral, and Sensitive**. This is shown in Figure 24.

Figure 24: *3 Main Data Categories*



The Data That Defines You

3 Main Categories of Personal Information

6

Ethan mentioned the main three groups of people aiming to acquire one’s data, either through buying or stealing: **companies, researchers, and cybercriminals**. Next, Ethan asked if students were familiar with the term **digital footprint**. One person had heard of it, and Ethan gave the definition (Figure 25).

Figure 25: *Digital Footprints*

Vocab - Digital Footprints



Information from <https://blog.saymine.com/blog-1/what-is-a-digital-footprint-exactly>

- The same way you leave footprints in the ground behind you when you walk, you leave a unique trail of data linked to your **IP Address** with **every** mouse click you make while using the internet

9

Following this, Ethan asked who had heard of a **VPN**. One person commented that it can keep your data safe and help someone change their location, and another responded they had

heard of it. He then presented three slides that discussed in depth what a VPN is, how to use it, and how it protects one's data. One of the three slides is pictured below in Figure 26.

Figure 26: *VPN Description*



The first slide explained fully what an **IP Address** is, who can see it, and how precise a location it shows for the user. The second slide pictured above shows how to use a VPN and how to connect to it, along with the result of what others see when you are connected, such as the new fake IP Address along with the fake location. The last slide of the set summarized the previous two, comparing a before and after of the IP address shown online by displaying an initial real location along with the fake one following the VPN connection.

The next few slides were composed of ones that asked the class what a **data leak** was and if they had ever heard of it. After getting some responses from the class saying **they hadn't heard of it**, Ethan and Kaley provided a definition to the students while testing them on some of the vocab terms brought up earlier. This was followed by an example of a data leak, specifically the University of California data leak on December 24, 2020, which exposed the email addresses, passwords, phone numbers, dates of birth, physical addresses, education levels, demographic information (ethnicity, gender, job history & title), and, most importantly, the social security numbers of every student attending along with all those who applied, emphasizing the severity of the issue. After clarifying why the topic was so important, the class moved onto a discussion recap where they mentioned some personal information of theirs that they should not give out online to see how much they learned since the last time the vocabulary was discussed. One person mentioned you **should not give financial info** such as pins or credit card details, and Ethan filled any of the students' gaps in knowledge.

The next part of the presentation introduced the idea of a **spam email** account, and explained its purpose in protecting your main email accounts from being in a data leak. This was followed by engaging the class with several examples Ethan shared of his personal and school

emails on a data tracker site, with the first slide showing the school email and confirming that it has not been in any data leaks. The next slide, however, showed the result of entering a personal email in potentially unsafe sites across the internet, shown in Figure 27.

Figure 27: *Pwned Example*

What Happens to the Spam Account?

- Checking my spam account that I use for most sites returned:

Oh no — pwned!
Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

- This means that my spam email account's **email** and **password** appeared in two separate data breaches
- These breaches are available online, and anyone could view the list and see your account information and use it to login to other websites that you may use the same passwords for
- If your info got leaked: **change your passwords**

19

This slide confirmed that Ethan's spam account was, in fact, involved in several data breaches, including what information was stolen because of it. Then, he discussed how a person can combat this if it happens to them. After this, another, more severe, example was presented, with an email connected to an University of California account that had been involved in 11 data breaches. This confirmed that every piece of information entered into the University of California website, including social security number, was stolen by hackers and released across the internet for anyone to see. Thus, the emails entered into the haveibeenpwned website showed how a lot of **sensitive info connected to the entered email was exposed**.

This presentation of important personal data being leaked was followed by an activity where the students **went onto the website themselves** and had the opportunity to test their own emails along with their parents to see for themselves if any of their information had been in a data leak. Along with having the students use the data tracking site, they were also shown a site that allows them to make temporary emails for website confirmation codes, which can keep them from using personal emails for different accounts for added safety and security. One student who had been hacked before asked a question about **what to do about an email that has been hacked** besides closing and deleting it, and Ethan explained that they should report it to Google as the company has better tools to track the perpetrator down.

The next section opened with a slide that discussed **AdBlockers** and gave several examples of some trusted ones, shown in Figure 28.

Figure 28: *Adblocker Description*

Minimizing Your Risk and Annoyances

Download an AdBlocker - remove bothersome ads and those with bad links trying to steal your info



Top AdBlockers:



22

This slide, along with its educational purposes, served as a gateway into discussing some **more serious topics**, such as the risks of being online. Ethan gave an activity where the students used the internet to **search his name** and where he goes to school (Ethan Reed, WPI) and then asked students to type in the chat what else they were able to find about him. Ethan explained that finding information about most people online is just as easy, and professionals can use this very maliciously. The last slide in this section discussed that there are many bad things on the internet, which someone can most likely find if they look hard enough, but that just because they can be found does not mean that they should be. Ethan also mentioned here that when trying something new or exploring different sites across the internet, the most important piece of advice is to **research beforehand** and to make sure that someone else has not had a negative experience with a certain website or account.

4.3.5.2 Personal Information Activities & Conclusion

The final slides consisted of an activity Ethan created and led called **Surfing Safely**, where he would give the name of a website, ask if it is trustworthy or not, and ask students what information they can and cannot give out. Four different websites were covered with the class, including a primary school math site, an educational site for all ages and subjects, a government social security site, and a tutoring help site. For each site, Ethan and Kaley let the class discuss whether or not the students trust it and what information they would give to it. Each site was covered in depth, explaining the correct answers to all of the questions after hearing the students' answers, and by the end the students seemed to have a very good idea of how to determine whether a site is trustworthy and what information, if any, could be given out. For the first site, there were **no responses**, but Ethan mentioned he would not give any of his data to it. For the next, several students said it was **trustworthy** in chat, and Ethan said he would give it some info,

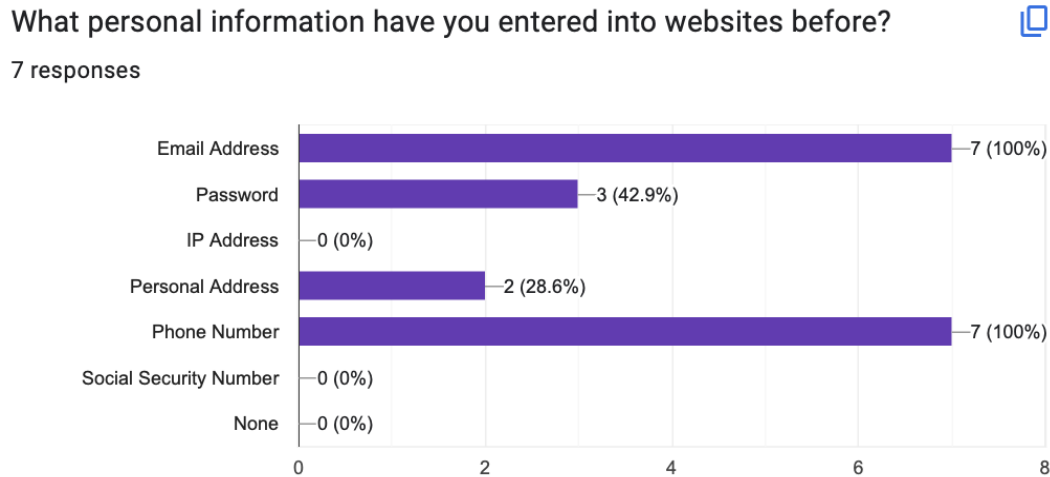
but not sensitive info. For the social security site, students said it was trustworthy in the chat **since it is a government website**. For the final site, students said it **looked suspicious**, and Ethan and Kaley agreed. Students performed very well in this activity, showing that they understood the material Ethan and Kaley aimed to teach.

4.3.5.3 Personal Information Results and Post-Evaluation Analysis

When asked at the end of the session whether there was any confusion concerning issues of personal security on the internet, several students responded that there wasn't and that the **lesson was pretty clear**. There were also those who were curious about **cybersecurity** who asked if there were any additional resources on it.

The pre- and post- evaluations for the Personal Information module showed a **great amount of information learned**, along with a **high overall satisfaction** rating for the presentation. Some examples of this include seeing that a great deal of students have entered sensitive information into sites before the lesson in the pre-evaluation, shown in Figure 29.

Figure 29: *Pre-evaluation Question Answers: What Personal Information Have You Entered Into Websites Before?*



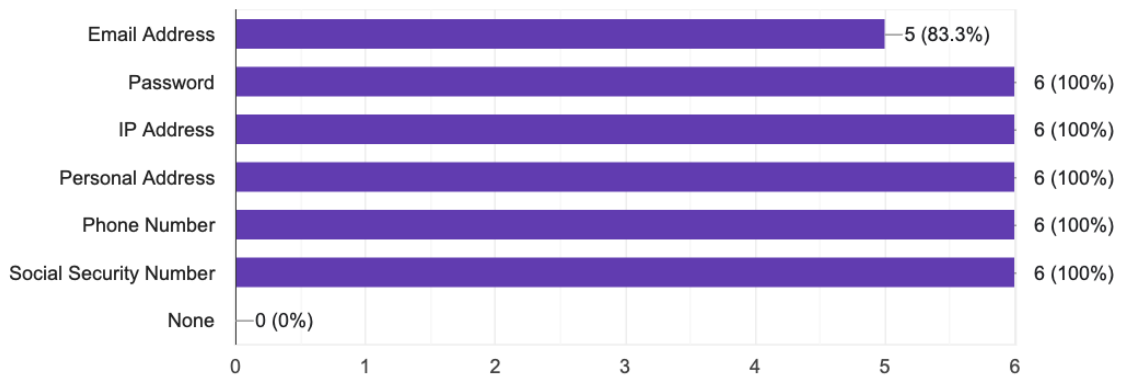
Most significantly, in the post evaluation, when students were asked about which of their information they will be careful about giving to sites in the future, almost all of them gave the **complete correct answer**, meaning the lesson taught them to be much more cautious online. The results are shown below in Figure 30.

Figure 30 : *Post-test Question Answers: What Personal Information Should You be Careful Of Entering Into Websites in the Future?*

What personal information should you be careful of entering into websites in the future?

 Copy

6 responses



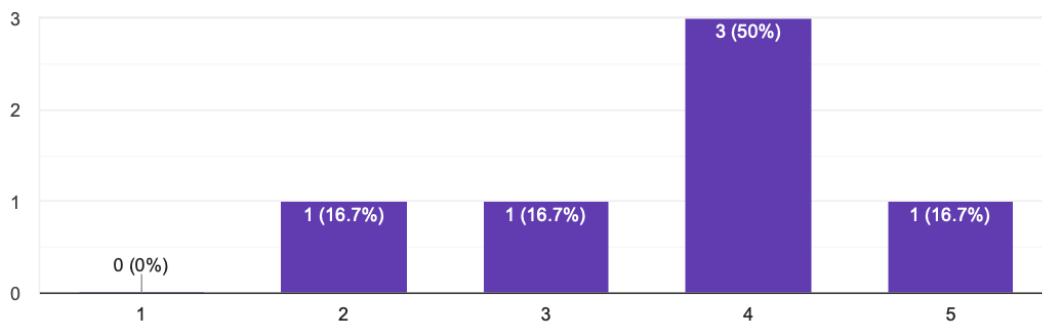
Not only did students learn a great deal, they also rated that the majority of the information that they learned was new, as shown in Figure 31.

Figure 31: *Post-test Question Answers: How Much of What You Learned Today was New for You?*

How much of what you learned today was new for you?

 Copy

6 responses



This shows that the lesson was effective at delivering its content, and students seemed to enjoy engaging with the material and asking questions, so the module seemed relatively successful. However, the amount of responses could have been bigger.

4.3.5.4 Recommendations for Personal Information Module

Although the post-evaluation responses were quite promising, there could have been **more results**. In the future, we would recommend encouraging more students to participate in the evaluations, and to run the module with more students to receive more data of its effectiveness. As discussion was also slightly scarce in this pilot, in part due to its virtual nature, we would recommend **utilizing the students' results** from their activities to spark some more discussion and encourage more people to share. With these recommendations, a better understanding of the curriculum's effectiveness can be established and more student enjoyment and participation can be encouraged.

5 Conclusion and Recommendations

In our research, we have found that Morocco's internet and computer access has **expanded very rapidly**, outgrowing its teaching infrastructure and leaving behind the subject of digital literacy. Morocco students seem to be struggling with the negative aspects of social media, in safely dealing with malware and other cyber attacks, and in thinking critically about information seen online. There have been efforts to increase digital literacy education in Morocco by the national government, UNESCO, and other organizations both local and foreign, but although they seem to have been beneficial overall, there is still more work to be done, especially regarding **educating children** about these important topics. Because of that, we worked with Educall to develop our digital literacy curriculum that can teach children about being safe online in a fun and engaging way. We divided our curriculum into five modules: **Misinformation, Personal Information, Social Media Safety & Mental Health, Cyberbullying, and Malware**, each addressing a unique problem that can be encountered on the internet. Each module is intended to last between two and three hours in one session, but can be easily expanded to last several sessions and even weeks. The curriculum was also adapted to be run both in physical and virtual classrooms for maximum usability. Pilots programs were run using all of the modules of the curriculum to test its effectiveness. The overall feedback from the pilots was that **student enjoyment** and the **amount they felt they learned were high**, but many pre- and post- evaluation results were made inconclusive as there were **not enough responses**.

Our recommendations include **adding extra reminders** for completing the pre- and post-evaluations, perhaps including a link that is constantly on screen for virtual sessions, so assessment results are better. For modules where formal pre- and post- evaluations did not seem to fit, implementing a different form of standardized knowledge testing for them in the future would definitely be beneficial for understanding their effectiveness. We also recommend **providing more time** for each module, depending on how much of the module an educator wants to cover and how in-depth they want the students to be able to discuss the content.

We intend for our curriculum to be easily understood and adapted by a wide variety of teachers to teach a wide variety of audiences. We are confident that Educall can use this curriculum to teach countless students about internet safety in the future, helping not just students but teachers and parents for years to come.

References

- Alaika, O., Doghmi, N., & Cherti, M. (2020). Social Media Addiction among Moroccan University Students: A Cross Sectional Survey. *PAMJ - One Health*, 1. <https://doi.org/10.11604/pamj-oh.2020.1.4.21930>
- Amdi, O. (2021, March 18). E-learning in Morocco: Excluding students in marginalized areas. SMEX. Retrieved March 2, 2023, from <https://smex.org/e-learning-in-morocco-excluding-students-in-marginalized-areas/>
- Baker, K. (2023, February 13). 10 most common types of cyber attacks today: CrowdStrike. *crowdstrike.com*. Retrieved February 25, 2023, from <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/>
- Bischoff, P. (2022, September 26). Which countries have the worst (and best) cybersecurity? *Comparitech*. Retrieved February 19, 2023, from <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>
- Bonnet, & Rosenbaum, J. E. (2020). “Fake news,” misinformation, and political bias: Teaching news literacy in the 21st century. *Communication Teacher*, 34(2), 103–108. <https://doi.org/10.1080/17404622.2019.1625938>
- Buckingham. (2015). Defining digital literacy - What do young people need to know about digital media? *Nordic journal of digital literacy*, 10(Jubileumsnummer), 21–35. <https://doi.org/10.18261/ISSN1891-943X-2015-Jubileumsnummer-03>
- Common Sense Education. (2014) Our K-12 Digital Literacy and Citizenship Curriculum. *Digital Literacy and Citizenship in a Connected Culture*. https://resources.finalsite.net/images/v1593155262/losalorg/hdwumjimrvmg3v5j1311/commonsense_digitalcitizenshipcurriculum.pdf
- DataReportal. (2023, January). *Countries with the highest internet penetration rate 2023*. Statista. Retrieved February 13, 2023, from <https://www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/>
- DigiGirlz [@digigirlzmorocco]. (n.d.). *Home* [Instagram page]. Instagram. Retrieved April 19, 2023, from <https://www.instagram.com/digigirlzmorocco/?hl=en>

- Distribution of e-commerce users in Morocco in 2021, by age group. Statista. (2022, May 4). Retrieved February 25, 2023, from <https://www.statista.com/forecasts/1306028/morocco-e-commerce-market-user-distribution-by-age>
- Educall. (n.d.). Educall. Retrieved April 19, 2023, from <http://educall.ma/wp/>
- Ghaudona, R. (2022, March 25). *Morocco - education and training*. International Trade Administration | Trade.gov. Retrieved February 13, 2023, from <https://www.trade.gov/country-commercial-guides/morocco-education-and-training-0>
- Glassman, A., & Sandefur, J. (2014, August 4). *Why African stats are often wrong*. Center for Global Development | Ideas to Action. Retrieved March 2, 2023, from <https://www.cgdev.org/blog/why-african-stats-are-often-wrong>
- Hanae, A. H. (2016). Media literacy education in English as a foreign language classroom. *International Journal of Media and Information Literacy*, 1 (2), 108-115. <https://cyberleninka.ru/article/n/media-literacy-education-in-english-as-a-foreign-language-classroom>
- Hanae, A. H. (2019). Media Literacy in Secondary School: Teachers' Attitudes. *Journal of Media Research*. 12. 10.24193/jmr.33.1. https://www.researchgate.net/publication/332119716_Media_Literacy_in_Secondary_School_Teachers%27_Attitudes
- Holden, G. (2021). *Wikipedia Launches Pilot Education Program for Digital Literacy in Moroccan Schools*. Morocco World News. <https://www.moroccoworldnews.com/2021/07/343278/wikipedia-launches-pilot-education-program-for-digital-literacy-in-moroccan-schools>
- Ibahrine, M. and Zaid, B. (2019) 'Spectrum management and democratization in Morocco', *Int. J. Information Technology, Communications and Convergence*, Vol. 3, No. 3, pp.191–208.
- Ismaili, J. (2020). Evaluation of information and communication technology in education programs for middle and high schools: GENIE program as a case study. *Educ Inf Technol* 25, 5067–5086. <https://doi.org/10.1007/s10639-020-10224-1>
- The World Bank. (2021). *Individuals using the internet (% of population) - morocco*. Retrieved February 11, 2023, from

<https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&locations=MA&start=1990&view=chart>

Jefferson, B. (2023, February 21). 15 common types of cyber attacks and how to mitigate them. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. Retrieved February 25, 2023, from <https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/>

Kaspersky. (2021). *Kaspersky Security Bulletin 2021. Statistics*. Kaspersky. Retrieved February 23, 2023, from https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf?o=7511/page/4/

Kemp, S. (2022, February 15). Digital 2022: Morocco - DataReportal – Global Digital Insights. DataReportal. Retrieved February 27, 2023, from <https://datareportal.com/reports/digital-2022-morocco>

Latrech, O. (2022, January 19). Digital: 9 out of 10 Moroccan children use smartphones. Morocco World News. Retrieved February 19, 2023, from <https://www.moroccoworldnews.com/2022/01/346627/digital-9-out-of-10-moroccan-children-use-smartphones>

Lieberman, A. (2017). *Terrorism, the internet, and Propaganda: A deadly combination*. Semantic Scholar. Retrieved February 13, 2023, from <https://www.semanticscholar.org/paper/Terrorism%2C-the-Internet%2C-and-Propaganda%3A-A-Deadly-Lieberman/6db18726f1ade13470872bafcecf06fcbd51022a>

Louragl, I., Ahami, A., Khadmaoui, A., Aboussaleh, Y., & Chaker Lamrani, A. (2019). Behavioral Analysis of adolescent's students addicted to Facebook and its impact on performance and Mental Health. *Acta Neuropsychologica*, 17(4), 427–439. <https://doi.org/10.5604/01.3001.0013.6550>

Miami, N., Belahcen, A., Lahlou, L., Abouqal, R., & ouanass, A. (2020). Cyberbullying in Rabat area Morocco: A middle school student survey. Research Square. <https://doi.org/10.21203/rs.3.rs-51636/v1>

Mouaziz, A., Byad, I. E., Sraoui, S., Biadi, M. E., & Moumni, J. (2023). Distance learning in Moroccan higher education during the COVID-19 pandemic: The case of Sidi Mohamed Ben Abdellah university students. *Arab World English Journal*, 13, 372–385. <https://doi.org/10.31235/osf.io/42j86>

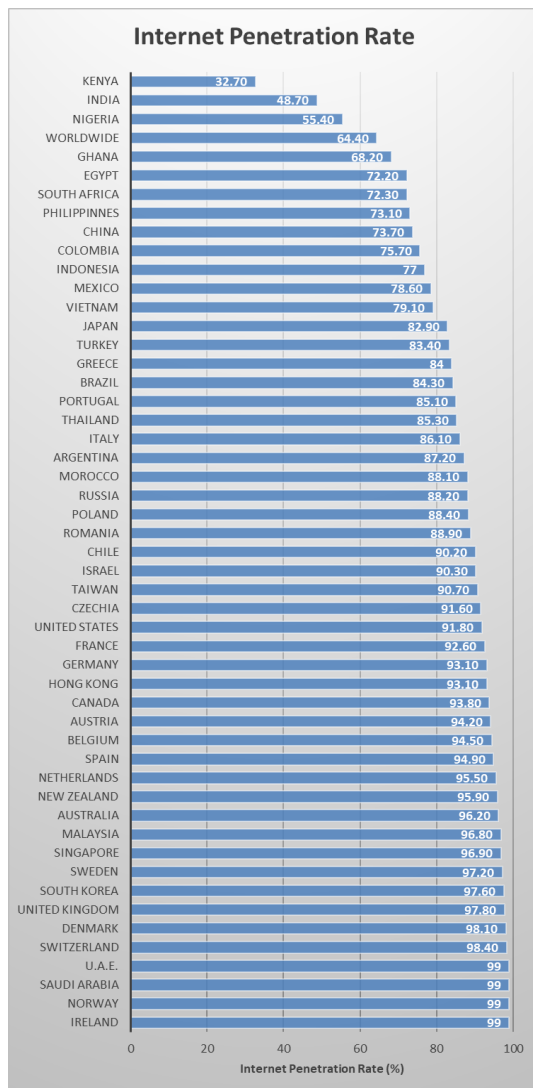
- Mrah, Isam & Tizaoui, Hicham. (2018). The Rise of Misinformation in the Digital Age: Moroccan Students' Attitudes and Perceptions of Fake News Online. *Journal of English Language Teaching and Linguistics*. 3. 10.21462/jeltl.v3i2.137.
- Nfissi, A. (2013). The state of the art of media and information literacy in Morocco. In U. Carlsson & S. H. Culver (Eds.), *Media and information literacy and intercultural dialogue* (pp. (87-96). The International Clearinghouse on Children, Youth and Media Nordicom University of Gothenburg.
https://gupea.ub.gu.se/bitstream/handle/2077/37328/gupea_2077_37328_1.pdf?sequence=1&isAllowed=y#page=89
- Patnaik, S. reading Wikipedia In the Classroom Final Report. In *Wikimedia Commons*.
https://commons.wikimedia.org/wiki/File:Reading_Wikipedia_Final_Report.pdf
- Rahhou, J. (2022, August 12). Morocco among 10 least Cybersecure countries for Digital Nomads. <https://www.moroccoworldnews.com/>. Retrieved February 1, 2023, from <https://www.moroccoworldnews.com/2022/08/350748/morocco-among-10-least-cybersecure-countries-for-digital-nomads>
- Raz, D. (2019, September 9). Youth in the Middle East and North Africa. Arab Barometer. Retrieved February 19, 2023, from <https://www.arabbarometer.org/2019/09/youth-in-the-middle-east-and-north-africa>
- Standerford, J. (2020, March 29). *Digital Literacy: Can You Spot the Fake?*. Licensed under CC BY 4.0. <https://www.oercommons.org/courseware/lesson/64650>
- Taylor, P. (2023, January 18). Morocco mobile cellular subscriptions 2000-2020. Statista. Retrieved February 26, 2023, from <https://www.statista.com/statistics/500993/number-of-mobile-cellular-subscriptions-in-morocco/>
- Reboot. (2022). *The most cyber-secure countries to work from*. Retrieved February 1, 2023, from <https://www.rebootonline.com/digital-pr/assets/most-cyber-secure-countries-to-work-from/>
- The SecDev Foundation. (2022). *Digital Safety Teaching Resources*. CyberSTAR.
<https://teaching.cyber-star.org/>

- The United Nations Educational, Scientific and Cultural Organization. (2022, March 25). *Morocco - Education and Training*. International Trade Administration. <https://www.trade.gov/country-commercial-guides/morocco-education-and-training-0>
- The United Nations Educational, Scientific and Cultural Organization. (2022, April 21). *How the GENIE Programme from Morocco is doing since receiving the 2017 UNESCO ICT in education prize*. UNESCO. <https://www.unesco.org/en/articles/how-genie-programme-morocco-doing-receiving-2017-unesco-ict-education-prize>
- United Nations Alliance of Civilizations. (2011, June 14). *The First International Forum on Media and Information Literacy (MIL)*. UNAOC. <https://www.unaoc.org/2011/06/the-first-international-forum-on-media-and-information-literacy-mil/>
- Wilson, C., Grizzle, A., Tuazon, R., Akyempong, K., Cheung, C. K. (2011). *Media and information literacy curriculum for teachers*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000192971>
- Wyndham School District. (2023). *K-8 Digital Literacy Curriculum*. Wyndham School District. https://cdn5-ss18.sharpschool.com/UserFiles/Servers/Server_27316100/Image/About%20WSD/Academics/Digital%20Literacy/WSD%20Digital%20Literacy%20Curriculum%20SB%20Approved%201-17-23.pdf
- Zaharia, A. (2023, January 10). The dangers of using public wi-fi (and how to stay safe). Aura. Retrieved February 25, 2023, from <https://www.aura.com/learn/dangers-of-public-wi-fi>
- Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021, February 10). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers*. Retrieved February 19, 2023, from <https://www.frontiersin.org/articles/10.3389/fpubh.2021.634909/full>

Appendices

Appendix A. Internet Penetration Rates of Selected Countries

Below displays the internet penetration rates of every country with a population of over 50,000 people. This data was provided by Statista (*Countries with the highest internet penetration rate 2023, 2023*).



Appendix B. Function of Common Malwares

Below is a table expressing the functions of some of the most common types of malware (Baker, 2023).

Malware	Function
Ransomware	A malicious user encrypts some or all of the information on a user's computer, holding it for ransom until a sum of money is paid.
Spyware	This will collect information about a user's web activity and report it to a malicious user.
Adware	Adware is a type of spyware that watches a user's activity and provides them with advertisements that are most relevant to them.
Worms	A worm is a program that can replicate itself and has the potential to spread throughout an entire network. They have the capacity to modify and delete files, inject more malware, duplicate themselves a lot to siphon memory and storage space, and other functions.
Rootkits	Rootkits give a malicious user direct control over an application on a computer, the whole computer, and even the entire network.
Scarewares	Scareware is often a malicious advertisement informing a user that their computer has been infected by malware, and offers them a way to download an "antivirus software." However, this "antivirus" is often actually another, more severe, malware.
Keyloggers	Keyloggers record every keypress or mouse click a user makes, then sends this information to a malicious user. This is often used to steal passwords.

Appendix C. Surveys

Appendix C1. Survey for Students

- General permission statements
- Demographic info
 - Age, gender
- General
 - How familiar are you with the term digital literacy?
 - Very familiar, familiar with some parts, unsure, sort of familiar, not familiar at all
 - What is digital literacy? (might be good to have just this free answer one)

- Some basic computer literacy demographics
 - Do you have a phone, computer, or tablet?
 - How familiar are you with technology?
 - How much do you use technology in school?
 - Which websites/tools are you familiar with or do you use?
 - Google
 - Yahoo/Bing
 - Amazon/Ebay
 - Wikipedia
 - Online news sites
 - Online calculator/math tools
 - Online question forums
 - Online game sites
 - Do you know what chatGPT is?
 - Browsing habits
- Social Issues
 - Do you use social media? (Y/N)
 - Which of the following have you put on social media: name, face, contact information, address/area of residence
 - Cyberbullying
 - Have you ever been involved in cyberbullying?
 - Do you know how to react when you are involved in or notice cyberbullying?
 - Are you familiar with the tools a website has to stop cyberbullying?
 - Are you familiar with the term “digital footprint”? (Y/N)
 - I always think twice before posting something on the internet
 - Highly agree, somewhat agree, neither agree nor disagree, somewhat disagree, highly disagree
 - I am cautious with my personal info?
 - Highly agree -> highly disagree
 - I am aware of what personal information is
 - I am familiar with why it is important to keep this information private
 - Once something is posted on the internet, it will stay on the internet in some form forever
 - Highly agree -> highly disagree
- Privacy and Malware
 - I am familiar with the ideas of malware and computer viruses
 - What are some ways that you could get a virus?
 - Short written response

- Which of the following steps do you take to protect your privacy on the internet or on your phone?
 - Privacy settings
 - 2Fa
 - Geotagging
 - Uninstall unused apps
 - Don't take all friend requests
- You can have absolute privacy while on the internet
 - Highly agree -> highly disagree
- Misinformation and Propaganda
 - Do you find out a lot about current events through the internet?
 - True or False: Anyone on the internet can post information that may be correct or false
 - I am able to distinguish if a source of information may be biased
 - Strongly agree -> disagree
 - How can you tell what information is true online?
 - Which of the following methods (if any) do you employ to verify a source online?
 - checking its author, date, what site it came from, the purpose of the content and if other sources back the information up
 - What sources provide the most accurate information?
 - Describe in a few words why?

Appendix C2. Survey for Teachers

General permission statements

- Demographic Information
 - Gender
 - Years of teaching
 - Subject taught
- How familiar are you with Digital Literacy?
- How familiar are your students/ how safe online do you think your students are online?
- Do you believe your school teaches children enough about digital literacy?
- How many of your students use social media?

Social Issues

- Do you use social media?
- Do you think students know not to put too much information, such as their name, face, contact information, or other personal information on social media?
- Cyberbullying

- Do you know how to react if someone is struggling with cyberbullying?
- Are you familiar with social media's cyberbullying protection mechanisms?
- Does the school teach students how to approach cyberbullying?
- How much critical thinking do you think students apply before posting something on the internet
 - A good lot -> none at all
- Once something is posted on the internet, it will stay on the internet in some form forever
 - Highly agree -> highly disagree
- My students are aware of what personal information is
- My students are familiar with why it is important to keep this information private
- How comfortable are you teaching about these topics?

Privacy and Malware

- Are you familiar with the ideas of malware and computer viruses?
- Do you know how to avoid downloading viruses?
- Do your students know how to avoid downloading viruses?
- Do you use an antivirus software?
- Do your students use an antivirus software?
- How much of your personal information do you think is on the internet?
- Which of the following steps do you take to protect your privacy on the internet or on your phone?
 - Privacy settings
 - 2Fa
 - Geotagging
 - Uninstall unused apps
 - Don't take all friend requests
 - Other: ____
 - None
- How comfortable are you teaching about these topics?

Misinformation and Propaganda

- Which sources do you get the news from?
 - TV/Newspaper
 - Website
 - Social Media
- I am able to distinguish if a source of information may be biased
 - Strongly agree -> disagree
- Which of the following methods (if any) do you employ to verify a source online?

- checking its author, date, what site it came from, the purpose of the content and if other sources back the information up
- What sources provide the most accurate information?
 - Describe in a few words why?
- Which of the following methods do you employ to verify a source online?
 - Short response? checking its author, date, what site it came from, the purpose of the content and if other sources back the information up
- How concerned are you about the radicalization of youth through the internet by terrorist organizations?
 - Very - > not at all
- Are your students familiar with terrorism?
- Does your school teach kids about the danger of terrorist groups?
- Do you think your school should teach more about it?
- How comfortable are you teaching about these topics?

Would you like to learn more about any of these topics? (Short response)?
If yes, what resources would you like to receive about them?

Appendix D. Interview Questions

Interview Questions Regarding Background:

- What do you think digital literacy is?
- Which areas require the most focus?
- What do you think are the consequences of a lack of digital literacy?
- What do you think the average level of digital literacy is in this school/program?

- How much do you think is known about social media and its mental health effects?
- How much do you think is known about cyberbullying?
- How much do you think is known about protecting privacy and security among students?
- How much do you think is known about malware among the students?
- How much do you think is known about misinformation and propaganda among students? What effect do you think this has?

- What are some ways students connect to you on a daily basis about the technology they use? Do you have any specific examples?
- What are some effects of technology on your students that you've noticed?
- What are some methods already being employed to teach digital literacy?
- What are some barriers to teaching digital literacy?
- What are some best practices for teaching digital literacy?

Regarding Curriculum:

- Thoughts and opinions?
- Rank the curriculum topics.
- Do you think this is appropriate for a 4th grade audience? How would you change it for younger / older grades?
- Thoughts on activities? Any additional suggestions for activities?
- Anything else you would like to suggest in general?

Appendix E. Curriculum Overview

Digital literacy involves the skills to navigate the internet safely and effectively, as shown in our diagram below. Digital literacy is vital for every user of the internet to be familiar with, because although the internet is incredible, there are also many dangers that come with it.



This digital literacy curriculum consists of five modules: Misinformation, Personal Information, Social Media & Mental Health, Cyberbullying, and Malware. Each module loosely follows a 6 step structure: **Goal & Objectives**, **Time & Materials**, **Introduction**, **Activities**, **Assessment**, and **Conclusion**. The **Goal & Objectives** section tells educators about what the module is trying to teach and the major learning outcomes expected from students. The **Time &**

Materials section tells educators how long the module should last assuming it is being completed in 1 session, as well as giving all of the materials and resources required to teach the module as written. The **Introduction** section asks students about their past experiences with the threats and how they dealt with them. It also introduces the major concepts and terminology in the module. The **Activities** section looks different for every module because activities will be more effective for some topics than others, and each module is intended to feel unique so few activities are repeated. This section includes how all of the material is taught and reinforced, and provides teachers with activities and slideshows that can be used to teach the material to students. The **Assessment** section is also unique to each module, sometimes consisting of gamified online quizzes and sometimes of complex scenarios to be discussed in small groups and shared with the class. The ultimate goal of this section is to allow educators to see what students have learned from the module and to correct any misconceptions or incorrect thoughts the students might have taken away from the module. The final section in each module is the **Conclusion**, in which the educator summarizes the major takeaways from the module, asks students what they learned or how their behavior will change in the future, and addresses any final questions or comments. Using this model of module sectioning seems standard across curriculums of many different topics, and it fits our curriculum as well.

This curriculum is also built in a relatively loose way, providing teachers with some activities and resources to teach the content, but not holding them to the provided structure. Because the educator using the curriculum knows their students the best, it is built to be easily modified to better fit the students. Each module is meant to provide between 2 and 3 hours of content in a single session, but it gives teachers the ability to easily add or remove some of the content to better fit a time limit, or even to stretch the given materials across multiple sessions over multiple weeks if desired. Giving educators this amount of freedom was important to us when designing the curriculum because not all classroom environments are the same and it is important to adapt any lessons to their needs.

This curriculum was originally built to be taught to the 4th graders at Vision School, and as such the material should be appropriate for children 9 years and older. However, because of our opportunity to work with students from DigiGirlz as well, the material was slightly modified to suit the high school age group, and converted into an online format. This makes the curriculum appropriate for students anywhere from 9-17 years old, and it can be taught in both physical and virtual classroom environments for maximum versatility.

Appendix F. Misinformation Module

Goal: For students to understand what misinformation is and techniques to recognize it

Objectives: Students will be able to

- Verify sources, including the type of source
- Identify which new articles are fake

- Understand what bias is

Total time: 60-80 minutes

Materials:

- Computer with internet access and projector
- Whiteboard and markers
- Kahoot.it

Introduction (20 minutes, presenters):

- Students will discuss whether they know what fake news and bias is along with how they make sure a source is trustworthy, and if they do, what platforms they use in small groups. On a whiteboard they will write what comes to mind.
- Create a word bubble with the word “fake news” at the center and have students raise their hands and list what comes to mind and have a discussion
- Have them reflect on what they know in regards to how trustworthy a source is and the effect is had when doing a project/paper
- Explain how this lesson will cover rules regarding verify resources along with identifying the legitimacy of a news source

Verify Resources (40 minutes, student activity):

- Techniques
 - 5 pillar of verification
 - Provenance: Are you looking at the original account, article or piece of content?
 - Source: Who created the account or article, or captured the original piece of content?
 - Date: When was it created?
 - Location: Where was the account established, website created or piece of content captured?
 - Importance to ensure accuracy of stories/Information
 - Helps to avoid amplifying fabricated news
 - Adds context, detail, history & transparency to the stories
 - Helped find clues and evidence to verify images, videos, and information
 - Activity: Give a bunch of stories about a topic and have the students break up into pair to discuss specific questions
 - <https://www.learningforjustice.org/classroom-resources/lessons/evaluating-online-sources>
- Bicycle Activity
 - <https://www.learningforjustice.org/classroom-resources/lessons/choosing-reliable-sources>

Fake News/Bias (20 minutes):

- Fake News
 - Goal: to falsely alter the reputation of a person or entity, or to make money out of it
- Bias
 - Types of Biases
 - Similarity Bias
 - Experience bias
 - Distance Bias
 - Safety Bias
 - <https://lifepointhealth.net/news/5-biases-that-impact-decision-making>
 - Activity: Give a scenario with factual evidence then write to opinion statements have the students discuss what type of bias it is and have them think if they ever had any type of biases

Closure (10 minutes):

- Have students review what they learned as a class, mentioning what they will do differently now when they look for sources
- Share final results with worksheets
- Ask students if they have any questions about fakes news/bias, verifying sources , or any of the questions covered in this lesson
- Remind students that if they are ever in doubt they should refer to a trusted adult
- End the lesson by thanking the students for their participation

Assessment:

- Assess worksheets to ensure they are completed
- Make sure students know how to verify resources and how to identify the legitimacy of a new/information
- Note: It may be helpful to inform parents and guardians about this lesson ahead of time so they can continue the conversation at home.

Vocabulary:

Misinformation	Creating of fictitious (fake) memories by providing misleading information about an event after it takes place
Fake News	Apps and websites that enable users to share content; youtube, twitter, facebook
Bias	To be against one person or group, especially
Fabricated	False, made-up
Anonymous	Not revealing one's identity
Legitimate	Lawful; authentic

Quiz:

<https://www.internetmatters.org/issues/fake-news-and-misinformation-advice-hub/find-the-fake/>
[Kahoot Quiz](#)

Flashcards:

https://quizlet.com/_d3g16o?x=1jqt&i=3bz02j

Appendix F1. Misinformation Module Assessment Questions and Answers

1. Which of these is the most reliable source?
 - a. Social Media Post
 - b. Magazines
 - c. Advertisements
 - d. Moroccan World News
2. What is disinformation?
 - a. False news/stories that are purposefully spread to create harm
 - b. News/stories that are true
3. What do you look for when verifying a source?
 - a. Intent/Purpose of the Article
 - b. All of the above
 - c. Bias
 - d. Author
4. Which part of an article should you NOT check?
 - a. Author
 - b. Intent
 - c. Headline
 - d. Date
5. What is the purpose of the media?

- a. To communicate with family and friends
 - b. To advertise or promote a product/service
 - c. To convey information
 - d. To have many followers and become an influencer
6. Misinformation is creating fake memories by providing misleading information about an event after it takes place.
- a. True
 - b. False
7. Which one of these is not a problem with the media?
- a. Lack of statistics
 - b. Opinion
 - c. Headlines are misleading
 - d. A lot of sources

Answers:

1. D
2. A
3. B
4. C
5. C
6. A
7. D

Appendix G. Personal Information Module

Objectives:

- Students will understand what personal information of theirs is collected by websites
- Students will be able to understand the importance of online privacy and why there is a market for their personal and digital data
- Students will be able to understand what a digital footprint is and how to minimize it

Expected Time Length: 1.5 hours

Materials:

- Computer with internet access and projector
- Whiteboards and markers
- Computers for students to check digital footprint on [site](#)

Introduction (20-30 minutes):

- Start by asking students what they know about personal information and data collection and have them write about what they think is available, what may be collected, and why
- Explain the importance of personal information and why it is collected online, along with the importance of protecting it
- Discuss digital footprints and how students can minimize the amount of personal info of theirs that is collected online

Personal information Demonstration and Activity

- Give students examples of others who have used emails for years, along with the effects of using these emails throughout several sites along with similar passwords
- Show several instances increasing in severity of different emails
 - Start with basic information stolen (usernames, passwords)
 - Work up to larger details (phone numbers, IP addresses, social security numbers)
- Explain the importance of each of the factors mentioned in the data leaks and why people are after them and what they can be used for
- Show how to prevent losing information like this in the future
 - Using VPN for security when browsing online
 - Different passwords for accounts being made to minimize effects of data leaks
- Explain that the annual data collection market is worth [over 20 billion Dirham](#) every year, and if people are willing to pay so much for it then it must be worth protecting

Scenario Discussion (20 minutes):

- Allow students to break into groups to complete activities regarding different types of individuals and their respective digital footprints
- Show the students how to use their new knowledge of information and privacy and how to determine which individuals would be most at risk after hearing from the groups their previous inferences or predictions

Activity (5-10 minutes)

- Students will use website to check if emails have been in data breaches
- Show severity of each data breach
- Students can use parents emails and check if they have been in breaches and explain what has been exposed from the leaks and how to protect and prevent against them in the future

Closure (5-10 minutes):

- Review what the students learned about the materials shown
- Leave time for any remaining questions that individuals may have regarding the main three topics
- Discuss digital footprint and finish with how to make sure you minimize the information that you leave about yourself online

Assessment:

- Assess the students' understanding by reviewing quizzes
- Ensure that each student is aware of how to act when they are using technology and surf websites online or create new accounts
- Students will have the opportunity to alter any old emails or passwords to be less susceptible to virtual attacks in the future

Introduction to Government Institutions

- [CNDP](#)
- How to react to getting data stolen
- [Law 0908](#)

Vocabulary:

Data Privacy	The relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.
Data Collection	The process of gathering and measuring information on targeted variables in an established system, which then enables one to answer relevant questions and evaluate outcomes.
Digital Footprint	One's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or digital devices.

Appendix H. Cyberbullying Module

Goals: For students to understand cyberbullying and how to handle it

Objectives:

- Students will be able to recognize an event of cyberbullying
- Students will know how to respond if they or someone they know is being cyberbullied.

Expected Time Length: 1.5 hours

Materials:

- Computer with internet access and projector
- Whiteboards and markers
- [Scenarios of cyberbullying](#), either printed or shown on a screen
- Video about cyberbullying

Introduction (20-30 minutes):

- Start by asking students if they know what bullying is and having them discuss it in small groups for 5-10 minutes. Let them share and write their responses on the whiteboard.
- Explain to them that bullying can happen online as well, and that it is called cyberbullying. Pass out the [best practices](#) for addressing bullying and cyberbullying or show them on a screen.
- Ask the students if they have ever seen cyberbullying or experienced it themselves, also in small groups, for 5-10 minutes.
- Explain that in this lesson, they will learn more about cyberbullying and what to do if they or someone they know is being cyberbullied.

Cyberbullying story (40 minutes):

- Show a video about cyberbullying to the students. Pause at various points to ask students about what they think about what is happening, what they would do, etc. Some possible time point stops are listed.

Option 1: <https://www.youtube.com/watch?v=GSE6spm-gyl>

1:13 What do you think is going to happen?

1:57 How do you feel about the characters so far?

2:24 What are your thoughts so far? What would you do in this situation?

3:25 Do you think this situation will escalate? How would you handle this?

4:18 How do you think Amy is feeling right now? What should she do to address this?

4:57 How do you think Amy is feeling? What would you do if you were her or her friend to address this?

5:25 How did the Amy's friend address the situation? Would you do the same?

6:12 How did that confrontation go? Do you think the issue was resolved? Would you change anything about how that went?

7:03 How

Option 2: <https://www.youtube.com/watch?v=tJsGGsPNakw>

0:44 What is the main character doing in the scene? What does she notice? What is the significance of the purple substance?

1:43 What's happening to the boy? What does the girl notice? What could be the repercussions of telling the counselor?

2:37 How does the entire school treat the girl after someone posted on social media what she reported? How is she feeling right now?

3:00 What is the significance of the question “are you okay?”?

3:13 What happened to the purple substance after asking about “are you okay?”?

3:47 What do you think of what the father said? Does he truly understand her?

4:36 How might the boy feel about all of the comments posted? What do you think might happen or what do you think he will do?

5:40 What might be the girl's intention in reaching out to the boy? And by reaching out, what might she have prevented?

7:00 By talking, do you think they each relieve some of the burden they each had felt? What is the key message to take away from this video?

- Explain to the students that cyberbullying can happen through text messages, social media, and online games. Ask the students how they would feel if they were the person being cyberbullied, and write their responses on the whiteboard.
- Discuss ways to prevent cyberbullying, such as not sharing personal information online, not responding to mean messages, taking a break from social media for a while, and telling a trusted adult if they see cyberbullying happening.

Scenario Discussion (20 minutes):

- Have the students form small groups, and distribute [scenarios](#) to each group, either on paper or projected on a screen. The students should discuss whether cyberbullying was occurring, what the characters did right and wrong, what the students would have done, how the students feel about the scenario.
- Have students share their answers with the class and discuss them as a group between each scenario.

Closure (5-10 minutes):

- Review what the students learned about cyberbullying.
- Ask students if they have any questions or concerns about cyberbullying.
- Remind the students that if they or someone they know is being cyberbullied, they should tell a trusted adult right away.
- Give out handouts with [resources](#) and hotlines that students can contact if they or someone they know is being cyberbullied.
- End the lesson by thanking the students for their participation and encouraging them to be kind to each other both in person and online.

Assessment:

- Assess the students' understanding of cyberbullying by reviewing how they responded to the scenarios and observing their participation during the discussion.

- Ensure that each student is aware of what to do if they encounter cyberbullying in the future.
- Note: It may be helpful to inform parents and guardians about this lesson ahead of time so they can continue the conversation at home.

Vocabulary:

Cyberbullying	Bullying through means of the internet, computers or mobile devices
---------------	---

Appendix H1. Cyberbullying Module Best Practices

How to Address Bullying

1. Respond firmly, but not with an insult or through fighting, and avoid the bully

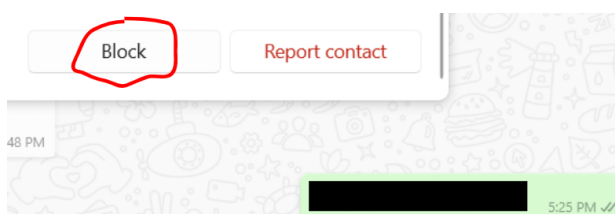
Bullies feel like they need someone weaker to pick on to feel more important or in control. By showing that you are not weak by firmly saying “Stop.” “Leave me alone.” or “Back off.”, or showing that they cannot affect you, they will stop bullying.

2. Tell a parent, teacher, or other trusted adult

Parents and teachers genuinely care about your well being, and they want to help you resolve any issues of bullying. Many teachers are trained to help you deal with your bully, and they will know how to help you without thinking any less of you. However, they can't help if they don't know about it, so make sure you share any bullying events with them!

How to Address Cyberbullying

1. Block Contact from the Bullies

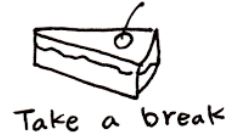


Bullies want to see a reaction from their victims, so just ignoring them is often effective enough at making them stop. Most social media platforms have features that allow users to stop seeing

messages from others, so take advantage of those to ignore the bully.

2. Take a Break from the Source of Bullying

Simply taking a break from the platform is often effective at ending cyberbullying for the same reasons as above. You won't have to see the messages, and the bully won't get a reaction and will eventually stop.



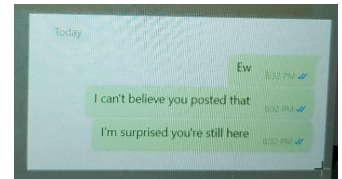
3. Don't Retaliate, it may Escalate the Bullying



Bullies want to see a reaction, so don't give them one. If you react, they'll keep bullying because they know they can hurt you, or the situation will escalate and you may say or do something you'll regret.

4. Take Pictures of the Messages or Posts

Adults and the social media companies themselves have the power to punish the cyberbully for their actions. By collecting evidence and pictures of the threatening actions, it is easier to talk to adults and social media companies about the issue, and it is easier for them to make the cyberbullying stop.



5. Tell a Parent, Teacher, or Other Trusted Adult



Parents and teachers genuinely care about your well being, and they want to help you resolve any issues of cyberbullying. Many teachers are trained to help you deal with your bully, and they will know how to help you without thinking any less of you. However, they can't help if they don't know about it, so make sure you share any cyberbullying events with them.

Stop Silence, an anonymous helpline for victims of bullying and mental distress: <https://www.stopsilence.net/>

Appendix H2. Cyberbullying Module Best Practices

1. Chafika is a high school student who is active on social media. She has been posting pictures and updates about her life on Instagram for a few years now and has built up a decent following. One day, she receives a direct message from someone she doesn't know. The message reads: "Hey Chafika, have you seen the latest meme about you? It's hilarious!"

Confused, Chafika asks the person what they are talking about. The person sends her a link to a meme that has been circulating on Twitter and Facebook. The meme is a photoshopped image of Chafika with a caption that makes fun of her appearance.

Chafika is shocked and hurt. She starts receiving more messages from people who have seen the meme and are laughing at her. Some of the comments are cruel and personal. They call her names and make fun of her weight.

Chafika feels embarrassed and ashamed. She tries to ignore the messages and delete the meme, but it keeps popping up on different platforms. She starts feeling anxious and depressed, and her schoolwork starts to suffer. She eventually confides in a friend, who helps her report the bullying to the school authorities and the social media platform.

However, the damage has already been done. Chafika's self-esteem had taken a hit, and she felt like she couldn't trust anyone online anymore. The experience has left her feeling isolated and vulnerable.

2. Sahdik was a college student who loved to play video games. He spent hours online, chatting with other gamers and honing his skills. He joined a website where he could talk to other people who loved video games as much as he did. At first, everything seemed great. He made a new friend, a girl named Sara, who gave him some good advice on how to play one of his favorite games.

But things quickly took a turn for the worse. Sara started acting weird and saying things that made Sahdik uncomfortable. She would send him messages late at night, even when he asked her to stop. She started telling other people on the website that they were in a relationship, even though Sahdik didn't want that. He tried to block her from talking to him, but she made new accounts to keep bothering him.

Sahdik felt really bad. He couldn't concentrate on his schoolwork, and he was afraid to go online. He didn't know what to do. He felt like he was being stalked and harassed by someone he thought was his friend.

One day, Sahdik decided to confide in a friend about what was happening. His friend listened to him and helped him tell the people in charge of the website what was going on. They took the matter seriously and banned Sara from the website. But even though Sara was gone, the damage had been done. Sahdik still felt scared and vulnerable. He felt like he couldn't trust people online anymore.

Sahdik's friend encouraged him to talk to a doctor about what he was going through. The doctor helped Sahdik understand that what had happened to him was not his fault, and that he deserved to feel safe and respected online. With the doctor's help, Sahdik was able to overcome his fear and start enjoying video games again.

3. Fama is a quiet, shy 5th grader who has always struggled to make friends at school. She spends a lot of time online and has made a few friends through social media platforms. Fama likes to post pictures of her artwork and writing online, hoping to get some positive feedback.

One day, a group of popular kids in her class find Fama's social media accounts and start leaving mean comments on her posts. They start calling her names like "loser" and "nerd" and telling her that no one likes her or her work. Fama tries to ignore them and keep posting, but the kids won't leave her alone.

The cyberbullying continues for weeks, with the popular kids leaving nasty comments on every post Fama makes. They even start creating fake accounts to make it look like other people are agreeing with them.

Fama feels like she can't tell anyone what's happening because she's afraid of making things worse. She starts feeling anxious and depressed and doesn't want to go to school anymore. She starts making excuses to stay home, pretending to be sick or saying she has to go to the doctor.

Her parents eventually notice that something is wrong and ask Fama what's going on. Fama finally tells them about the cyberbullying, and her parents talk to the school principal about the situation. The school works with Fama's parents to track down the kids who were cyberbullying her and they are given consequences for their behavior.

While the cyberbullying stops, Fama still feels hurt and embarrassed by what happened. She starts seeing a counselor to help her work through her feelings and build her confidence. Over time, Fama learns to use social media in a safer and more positive way and she starts feeling more positive about herself and her place in the world.

4. Tamra is a 14-year-old girl who loves making TikTok videos with her friends. She spends hours filming and editing videos, trying to make them as funny and entertaining as possible. Tamra loves getting likes and comments on her videos, and dreams of becoming a famous TikTok star.

One day, Tamra posts a video that features her and her friends dancing to a popular song. She thinks it's funny and creative, and is excited to see how many likes and comments it will get. But as soon as she posts the video, she starts getting mean comments from other TikTok users.

People start leaving comments calling Tamra and her friends ugly, fat, and stupid. They start making fun of their dancing and telling them to stop embarrassing themselves. Tamra feels hurt and embarrassed by the comments, but doesn't want to delete the video because she thinks it's good.

The cyberbullying continues for days, with people leaving mean comments on all of Tamra's videos. Some people even start creating fake accounts to harass her even more. Tamra feels like she can't escape the bullying, even when she logs off of TikTok.

Tamra tells her parents about the cyberbullying and they help her report the abusive comments and accounts to TikTok. The company takes action and removes the abusive comments and accounts from Tamra's page. They also work to prevent future cyberbullying by implementing stronger security measures and stricter policies.

Tamra feels better knowing that the bullying has stopped, but she's still wary of posting new videos on TikTok. She learns to be more careful about what she posts online and to never let other people's opinions bring her down. Tamra continues to make TikTok videos with her friends, but now she does it because it makes her happy, not because she wants to be famous.

5. There was a young man named Hassan who loved spending his time online. He was a talented gamer and enjoyed engaging with others on social media. One day, Hassan came across a user who made a comment that he disagreed with. Instead of ignoring it, Hassan decided to respond with a harsh comment, and thus began his journey into cyberbullying.

Hassan continued to attack this user online, leaving comments that were hurtful and derogatory. He would make fun of the user's appearance, criticize their opinions, and encourage others to join in on the bullying. Hassan also began to create fake accounts to impersonate the user and spread false rumors about them. As time went on, Hassan's attacks became more frequent and more aggressive, leaving the other user feeling isolated and afraid to engage online.

One day, Hassan received a private message from someone he had never met before. The message was from the parent of the user he had been cyberbullying, and it described the devastating impact that Hassan's actions had on their child. The parent explained how their child had become withdrawn and anxious because of the bullying, and how it had affected their schoolwork and personal relationships.

This message hit Hassan hard, and he began to realize the full extent of the harm he had caused. He felt ashamed of his behavior and guilty for not considering the consequences of his actions. Hassan reached out to the person he had been cyberbullying and apologized for his behavior. He also made a commitment to change his ways and to speak up against cyberbullying whenever he saw it happening online.

Over time, Hassan's online behavior improved, and he became an advocate for kindness and positivity online. He realized that it was easy to get caught up in the negativity of the internet, but it was important to remember that there were real people behind the screens, and that their words could have a lasting impact. Hassan learned an important lesson about the power of words and how they can be used to build up or tear down.

6. Zineb and Nadia had been friends since 1st grade. They were inseparable, spending countless hours together and sharing their deepest secrets. But as they grew older and entered high school, things began to change.

Zineb noticed that Nadia had become increasingly critical of her online. Nadia would leave mean, sarcastic comments on Zineb's Instagram posts, make fun of her in group chats, and publicly shame her for her appearance. Zineb tried to ignore it, thinking that Nadia was just going through a phase or was stressed out about school.

But things only got worse. Nadia started to send Zineb private messages that were cruel and hurtful. She would insult Zineb's intelligence, mock her interests, and she even threatened to reveal embarrassing secrets. Zineb felt like she was being attacked from all sides and didn't know what to do.

Zineb tried to talk to Nadia about how her behavior was affecting her, but Nadia brushed her off and accused her of being too sensitive. Zineb began to dread going online, knowing that there would be another attack waiting for her. She felt like she had lost her best friend and didn't know how to fix the situation.

One day, Zineb decided to reach out to a school counselor for help. The counselor listened to Zineb's story and offered her support and resources. Zineb also confided in her parents, who helped her to block Nadia on social media and encouraged her to spend time with other friends.

Zineb realized that it wasn't her fault after talking with the school counselor and confiding in her parents. They listened to her story and reassured her that she had done nothing wrong. The counselor helped Zineb understand that cyberbullying is never the victim's fault, and that Nadia's behavior was a reflection of her own issues, not anything Zineb had done. Zineb's parents also provided her with support and encouragement, which helped her see that she deserved to be treated with kindness and respect. By talking with trusted adults who cared about her, Zineb was able to see the situation from a new perspective and begin to heal from the harm that had been done to her. She made new friends, pursued her interests, and learned to be proud of who she was. Zineb also made a commitment to speak out against cyberbullying and to support others who may be going through similar experiences.

In the end, Zineb was able to overcome the hurt and trauma of cyberbullying, and she emerged stronger and more resilient than ever before. She learned an important lesson about the power of friendship and the importance of standing up for oneself in the face of adversity.

Appendix I. Social Media Module

Goals: For students to understand how to safely navigate social media, that their actions on the internet have consequences and the impact the internet can have on their mental health

Objectives:

- Students will learn about what social media is and how to stay safe on it
- Students know what to do if they receive suspicious messages or harassment
- Students will be able to recognize signs and symptoms of negative effects of social media on mental health

Expected Time Length: 1.5 hours

Materials:

- Computer with internet access and projector
- Whiteboard and markers
- Paper and markers
- [Online Interaction](#), [Netiquette](#) and [Mental Health](#) worksheets for lesson

Introduction (20 minutes):

- Students will discuss their views on social media, and if they do, what platforms they use in small groups. On a whiteboard in the front of the room they will list the social media sites they most commonly use
- Students will discuss in groups of 3-5 about their perceptions on social media and its positive and negative effects, demonstrating what they know in regards to social media, social media safety and effects on mental health. They will then share what they discussed with the class, which will be listed on a whiteboard at the front of the class.
- Explain how this lesson will cover rules regarding social media safety, etiquette, and mental health effects

Lesson and Activities (60 minutes):

- Safety
 - Who you interact with online, don't give out personal information
 - Name, address, school, age, phone number, email, photos with your house/neighborhood in the background, whether you're on vacation
 - Have students list out as many as possible before revealing the answer
 - Burger King Foot Lettuce:
https://www.youtube.com/watch?v=5IJ_234g4Ac
 - Removing EXIF data:
<https://lifehacker.com/what-is-exif-data-and-how-to-remove-it-from-your-photo-1845292669>

- Other ways to find location through images:
 - Google reverse image search
 - Reflections in glasses, windows, screens
 - Visual clues - if you take a picture near your house
- Activity: Given a photo, have students find where it was taken (or have students look at the metadata of a photo they have or are provided)
- Activity: Give a scenario of a person you encounter online, discuss in small groups and each group fill out the online interactions worksheet - then go over worksheets as a class
 - Sketchy spam
 - Random dms or friend requests
 - Online friend who suggests meeting up
 - Group chats and online forums
 - Being sent inappropriate content, who to go to
- People who will take advantage of you
 - Internet Predators - people on the internet with malicious intent to use or harm younger people
 - Grooming - Strategy a predator uses to slowly get closer to a victim with the end goal to use or harm them
 - Strategies groomers and predators use
 - Pretend to be someone they're not
 - Get you to trust them slowly - flattery, claiming to share interests
 - Try to isolate you from friends and family
 - Share inappropriate content
 - Get you to meet them in person
 - Threaten you - claim to have information about you or be able to hurt you
 - Examples:
 - <https://universe.byu.edu/2021/11/17/internet-vigilance-can-protect-children-teens-from-online-predators/>
 - Scroll down to image gallery, point out flattery, gifts, and isolation (photos 4, 6, 7, 8)
 - Forum and group chat dangers
 - Toxicity and dogpiling
 - Favoritism
 - Irresponsible moderators
 - Ignoring inappropriate behavior
 - Encouraging a toxic mindset - many mental illness related forums
 - Parasocial relationships - one sided relationships with celebrities online
- Recommend that students discuss with your parents about what they do online and keep them aware
- Netiquette
 - What you put on the internet reflects your character and stays there forever

- The effects of anonymity and how that doesn't justify being bad, respect people's privacy and don't leak things publicly without permission
- Follow etiquette you follow in real life
- Read before asking
- Present the best side of yourself
- Respect privacy
- Be respectful! Regarding identities, beliefs, being nice in general
- Keep in mind that tone is hard to convey through text
- Hate speech
 - How to handle and report it to an adult or website
- Activity: Fill out netiquette worksheet in small groups
- Activity: Create a brochure describing netiquette and why it's important
- Mental Health
 - Addiction
 - Symptoms: Spending more than 3 hours on social media per day, feeling restless without social media, ignoring real life, becoming stressed about likes/comments
 - Effects: low self-esteem, isolation, sleep-deprivation, helps fuel depression, anxiety
 - Social media is designed to be addicting - use allegory of junk food or candy - activates dopamine, which is the same chemical that keeps you wanting more of a food
 - Young people are especially susceptible since their brains are still developing
 - How to deal with it: talk to parents, set boundaries, limit use at dinner table, turn off notifications
 - Photoshop and idealization
 - Explanation of photoshop; ask if they are familiar with the concept
 - Photoshopping process video: <https://www.youtube.com/watch?v=iYhCn0jf46U>
 - Can also apply to guys
 - Filters
 - People choose what side of them to put on the social media - usually more perfect than reality
 - Social media feedback as validation
 - Activity: Give an example of a person who uses social media and have students state whether it is having a negative effect on their life or what they should do (Mental Health Scenarios worksheet)
 - Activity: Have students write down a list of rules and affirmations for themselves regarding how much and in what ways they will use social media

Closure (10 minutes):


- Have students review what they learned as a class
- Share final results of worksheets

- Ask students if they have any questions about social media, mental health, or any of the questions covered in this lesson
- Remind students that if they are ever in doubt they should refer to a trusted adult
- End the lesson by thanking the students for their participation

Assessment:

- Have students complete quiz assessment
- Assess worksheets to ensure they are completed
- Make sure students know how to be safe on social media and are aware of the potential mental health effects
- Note: It may be helpful to inform parents and guardians about this lesson ahead of time so they can continue the conversation at home.

Vocabulary:

<p>Social Media</p>  <p>"Social Media Icons With Paint Splash Effect" by Lewis Ogden is licensed under CC BY 2.0</p>	<p>Apps and websites that enable users to share content; youtube, twitter, facebook</p>
<p>Mental Health</p>	<p>Mental well-being</p>
<p>Photoshop</p>	<p>Program for editing photos</p>
<p>Netiquette</p>	<p>Rules for how to act respectfully on the internet</p>
<p>Toxic Environment</p>	<p>A environment (surrounding, condition) where bad things are considered normal and part of the group's behavior</p>

Quiz:

https://docs.google.com/forms/d/e/1FAIpQLSfxYZT3zJ7UBLhulXEDeGK4BbwuThVkkvPGfVg_eHM0zh-Ezg/viewform?usp=sf_link

Appendix J. Malware Module

Goal: For students to understand what malware is and how it generally works

Objectives: Students will be able to

- Define and recognize various types of malware
- Understand the potential risks and consequences associated with each type
- Safely avoid being attacked by them.

Total time: ~2 hours

Materials:

- [Pre-test and post-test](#), either printed or accessible online
- [Presentation slides](#) or some other way to present the course content
- [Handouts](#) on types of malware
- [Assessment](#) game materials

Introduction (10 minutes):

- Ask students to complete the Pre-test. It should not take longer than 5 minutes.
 - <https://www.opinionstage.com/page/ca14c681-7adc-49de-a819-aae3679a5017>
- Define what malware is: malicious software designed to damage or disrupt computer systems, steal information, or gain unauthorized access to a network.
- Discuss why malware is a problem and how it can affect individuals and organizations.
- Ask students if they have any experience or knowledge about malware in real life or in TV, movies, etc.

Direct Instruction (50 minutes):

- Present a slide deck that provides definitions and examples of each type of malware. The slide deck is built asking students to guess the function of each type of malware using pictures and to ask what students would do if they see the scenario. Teachers can also ask students why a hacker might want someone to install each type of malware.
- Provide students with a printed copy of the list of vocabulary, and go through pronunciation and definition of each term.

- Discuss how each type works and what risks and consequences are associated with them.
- Use both real-world examples and descriptive prognosis of virus attacks to illustrate the impact of malware attacks.

Vocabulary Practice (10 minutes):

- Distribute a [vocabulary sheet](#) to each student.
- Ask students to work in pairs or small groups to match each type of malware with its corresponding example scenarios of its function
 - https://quizlet.com/_d531m0?x=1jqt&i=3bz02j
- Review the answers as a class and clarify any misunderstandings or questions.

Assessment Project (10-30 minutes based on group progress):

- Divide students into teams and provide each team with several [cybersecurity-compromising tasks](#) that they can choose between (figure out how much money is in a person's bank account, determine a person's favorite food using spyware, etc)
- Ask students to play the role of hackers and use their understanding of malware to accomplish that task.
- Ask students to use at least three of the malware discussed to accomplish their task
- Have a teacher go around and ask how each group is doing, giving small hints and questioning logical decisions, and reiterating that doing these things is morally wrong
- Have students present their scenarios and solutions to the class in a short 3 minute presentation.

Conclusion (15 minutes):

- Go through the Kahoot to see how much information the students retained.
 - <https://create.kahoot.it/share/malware-post-lesson/7c06ba6f-27d1-4289-bfcf-a8f94a2ac384>
 - Explain why the right answer is correct if a large portion of the class was wrong and guide the class towards better understanding the question.
 - The questions can also be administered through other ways if you would prefer.
- Summarize the key takeaways from the lesson.
- Brainstorm with the class a few ways to stay safe from downloading malware.
- Encourage students to practice safe computing habits, such as avoiding suspicious websites, using antivirus software, and keeping their operating systems and applications up to date.
- Thank students for their participation and ask if they have any remaining questions or concerns.

Vocabulary:

Malware	Function
Malware	Software that seeks to damage, disrupt or get unauthorized access and information from a computer system
Viruses	When run by a user, a virus can replicate itself by modifying other computer programs and inserting its own code into those programs.
Worms	A worm is a program that can replicate itself and has the potential to spread throughout an entire network. They have the capacity to modify and delete files, inject more malware, duplicate themselves a lot to siphon memory and storage space, and other functions.
Antivirus	Protects a computer from malware by preventing the installation of malware and removing malware that has been installed.
Encryption	Converts the information on a computer into an unusable form that is very hard to revert without a special "key".
Ransomware	A malicious user encrypts some or all of the information on a user's computer, holding it for ransom until a sum of money is paid.
Spyware	This will collect information about a user's web activity and report it to a malicious user.
Adware	Adware is a type of spyware that watches a user's activity and provides them with advertisements that are most relevant to them.
Rootkits	Rootkits give a malicious user direct control over an application on a computer, the whole computer, and even the entire network.
Keyloggers	Keyloggers record every keypress or mouse click a user makes, then sends this information to a malicious user. This is often used to steal passwords.
Cryptojacking	Hackers take control of a user's computer and use its resources to mine cryptocurrency.
Scarewares	Scareware is often a malicious advertisement informing a user that their computer has been infected by malware, and offers them a way to download an "antivirus software." However, this "antivirus" is often actually another, more severe, malware.
Malvertising	Advertisements that, when clicked, install malware.
Trojans	Malware that is installed with another program or looks like a normal program, and when that program is run by a user, the malware is also run.
Phishing	Using fake communications to deceive a user and make them give up personal information, click a link, or download malware.

Appendix J1. Malware Module Assessment Questions and Answers

1. What is malware?

- a) A type of computer virus
- b) A type of computer program that is used to steal sensitive information
- c) A type of hardware device that can infect your computer
- d) None of the above

2. Which of the following is not a type of malware?

- a) Trojan
- b) Spyware
- c) Antivirus
- d) Adware

3. What is phishing?

- a) A type of malware that infects your computer
- b) A technique used by hackers to steal sensitive information
- c) A type of firewall
- d) None of the above

4. What is the best way to avoid malware?

- a) Download and install antivirus software
- b) Use a strong and unique password
- c) Keep your software up to date
- d) All of the above

5. What is ransomware?

- a) A type of malware that encrypts your files and demands payment to unlock them
- b) A type of malware that deletes your files
- c) A type of malware that steals your sensitive information
- d) None of the above

6. What is a rootkit?

- a) A type of malware that provides unauthorized access to your computer
- b) A type of malware that places advertisements all around your computer
- c) A type of system that protects against malware
- d) None of the above

7. What should you do if you suspect that your computer has been infected with malware?

- a) Ignore it and hope it goes away
- b) Run a scan with an antivirus software
- c) Click on the pop-up ads that appear on your screen
- d) None of the above

8. What should you do if you receive an email from an unknown sender with an attachment?

- a) Open the attachment to see what it is
- b) Delete the email and attachment immediately
- c) Forward the email to your friends to see if they know the sender
- d) None of the above

9. Which of the following is a strong password?

- a) Password123
- b) tO0*m?s#vQ
- c) 123456
- d) [Name of Website]!

10. Which type of malware is designed to monitor your internet activity and steal sensitive information?

- a) Trojan horse
- b) Worm
- c) Spyware
- d) Ransomware

11. What is the difference between viruses and worms?

- a) Viruses require human interaction to spread, while worms can spread automatically
- b) Viruses infect files, while worms infect networks
- c) Viruses are more dangerous than worms
- d) There is no difference between viruses and worms

12. What is the most common way for malware to infect your computer?

- a) By opening email attachments from unknown senders
- b) By visiting trusted websites
- c) By connecting to public Wi-Fi networks
- d) None of the above

13. What is a strong password?

- a) A password that is easy to remember
- b) A password that you use in a lot of places
- c) A password that you share with others
- d) A password that contains a mix of uppercase and lowercase letters, numbers, and symbols

14. What is a phishing email?

- a) An email that tries to trick you into revealing sensitive information
- b) An email that contains a virus
- c) An email that contains urgent information

d) Both A and B

15. What is a pop-up ad?

- a) An advertisement that appears in a separate window or tab
- b) An advertisement that contains malware
- c) A way for hackers to gain access to a computer
- d) None of the above

16. What is the purpose of antivirus software?

- a) To prevent hackers from accessing your computer
- b) To detect and remove malware from your computer
- c) To encrypt your files
- d) All of the above

17. What is data encryption?

- a) A way for hackers to gain access to a computer or network
- b) A type of antivirus
- c) A type of malware that spies on a users data
- d) None of the above

18. What should you do if you receive an email from an unknown sender?

- a) Open the email and respond to it
- b) Delete the email and don't respond to it
- c) Forward the email to your friends to see if they know the sender
- d) None of the above

19. Which of the following is a way to avoid downloading malware?

- a) Clicking on every link you find online
- b) Downloading software from reputable sources only
- c) Sharing your passwords with others
- d) None of the above

20. What should you do if you are unsure about whether a website or software program is safe to use?

- a) Use a search engine to find reviews and ratings from other users
- b) Ignore your concerns and continue using the website or software program
- c) Download the website or software program to a different device to test it out
- d) None of the above

Answers:

1. B
2. C
3. B
4. D
5. A
6. A
7. B
8. B
9. B
10. A
11. C
12. A
13. D
14. D
15. A
16. D
17. D
18. B
19. B
20. A

Appendix J2. Malware Module Scenarios and Solutions

1. Mohamed lost his Facebook account when a hacker broke into his account and changed his password. He is trying to figure out what he did wrong. With your new knowledge of malware, can you help him figure out what happened?

A couple days ago, he was checking his emails on his computer when he saw one that said he was charged 400 MAD for a purchase he didn't remember making. The email was poorly worded, with several typos, and it also said it had a link to the receipt for his purchase. He clicked the link, which downloaded a pdf file. He opened it and it brought up a real-looking receipt. Do you think he did anything wrong? What should Mohamed have done?

Later, Mohamed logged into his Facebook account on the same computer. He browsed through it for a few minutes, then he logged out. The following morning, he tried to get into his Facebook

account account, but it said that his normal password was wrong. How do you think this happened?

The intended answer is that Mohamed clicked a link from a phishing email and installed a trojan. Mohamed should have been more suspicious of the email and investigated it more before clicking the link. This trojan also came with a keylogger or rootkit, which allowed a hacker to steal Mohamed's Facebook password, then log in as him and change his password.

2. Nadia was reading an article and saw an advertisement for a cute blouse. She clicked the advertisement and it brought her to the company site. She looked for a few minutes, then left the site. Throughout the next few weeks, Nadia noticed that her computer was getting slower and that there were starting to be more advertisements on the websites she was visiting. Her computer was also opening new browser tabs that showed advertisements. She is starting to be concerned, what do you think happened?

She is worried that her computer is a lot slower than it used to be, and all of the advertisements are really annoying her. Can you think of any way to help her solve her problem?

The intended solution is that when Nadia clicked the link, it installed adware on her computer. This started loading a lot of advertisements onto her computer, which made it a lot slower. As time passed, the problem became worse and worse. The way to correct this is for Nadia to install an antivirus software to help her remove the malware, or for her to go through all of the programs on her computer and uninstall any program that looks suspicious.

3. Your friend Youseff is very concerned about having his money stolen by computer hackers. He has heard of a few different ways that hackers can use to take money from someone. Using what you know about malware, can you come up with three ways a hacker might be able to gain access to someone's bank account or take their money?

Intended answers include using ways to break into a bank account like keyloggers, rootkits, and even spyware, but other answers include ransomware and potentially cryptojacking.

Appendix J3. Malware Module Vocabulary

Malware	Function
Viruses	When run by a user, a virus can replicate itself by modifying other computer programs and inserting its own code into those programs
Worms	A worm is a program that can replicate itself and has the potential to spread throughout an entire network. They have the capacity to modify and delete files, inject more malware, duplicate themselves a lot to siphon memory and storage space, and other functions.
Antivirus	Protects a computer from malware by preventing its installation
Ransomware	A malicious user encrypts some or all of the information on a user's computer, holding it for ransom until a sum of money is paid.
Spyware	This will collect information about a user's web activity and report it to a malicious user.
Adware	Adware is a type of spyware that watches a user's activity and provides them with advertisements that are most relevant to them.
Rootkits	Rootkits give a malicious user direct control over an application on a computer, the whole computer, and even the entire network.
Keyloggers	Keyloggers record every keypress or mouse click a user makes, then sends this information to a malicious user. This is often used to steal passwords.
Cryptojacking	Hackers take control of a user's computer and uses its resources to mine cryptocurrency
Scareware	Scareware is often a malicious advertisement informing a user that their computer has been infected by malware, and offers them a way to download an "antivirus software." However, this "antivirus" is often actually another, more severe, malware.
Malvertising	Advertisements that, when clicked, install malware
Trojans	Malware that is installed with another program or looks like a normal program, and when that program is run by a user, the malware is also run
Phishing	Using fake communications to deceive a user and make them give up personal information, click a link, or download malware

