Proposal for Educating Children About Cybersecurity
Taryn Gilbert
CYSE 494

Problem: With technology such as smartphones, tablets, laptops, and smart watches rapidly increasing, it is important that children and teenagers know the dangers associated with the Internet and practice healthy habits to stay safe online. Although it may seem that malware attacks and hacking may only happen to adults, children and teens are mostly targeted on video sharing sites, chat rooms, and social media because of their lack of knowledge and experience on the Internet. According to a survey conducted about Internet Crime and Abuse, 86% of females surveyed said that they could chat online without their parent's knowledge and 54% said that they could have a cyber relationship (GuardChild, 2019). Setting up Parental Controls is a smart way to keep children off of dangerous websites, but it doesn't teach them why they are dangerous. While teaching children that you shouldn't do x, y, or z on the Internet, habits need to be made so that children are practicing these measures, not just learning about them.

Context: Children and teenagers not being educated about the Internet is a continuous problem that has serious consequences. According to the Center for Missing and Exploited Children, "Only 33% of households with Internet access are actively protecting their children with filtering or blocking software" (SentryPC, 2018). It is important for parents to protect their children, but it should also be the responsibility of the user to be educated on cyber issues. The research of 2278 teens and pre-teens conducted by the office of the Children's E-Safety Commissioner showed that 39% of children as young as eight, who use social media, have shared their real surname on their accounts, 24% have posted a photo of their school or school uniform and 8% have shared their phone number and/or street address (Office of the Children's eSafety Commissioner, 2016). Sharing this type of information on the Internet puts not only children, but anyone who shares this type of information at risk. Julie Inman Grant of Children's E-Safety Commissioner touched on this topic by stating, "Revealing information like your phone number, street address or school details on social media can expose children to a range of risks they may not have the maturity, judgment or resilience to handle on their own. In the rare or worst-case scenario, school details can also be used by online predators to find a child's location, to befriend a child or trick them into believing they know them" (Grant, 2016).

Solution: In order to educate children on staying safe on the Internet, I believe the solution is to create a smartphone application (APP) that teaches children and teens how to be safe on the Internet by acting as a virtual machine and displaying pop-up messages when users enter social media sites, view emails, play online video games, and use video streaming sites. All emails, video sharing sites, online games, and social media accounts will be accessible through this APP. When a user uses these apps, pop-up messages will appear which will give advice and tips on what to do, what not to do, or what to click on and what not to click on. For example, if a user were to open an email on this application that said they won a free vacation and to enter their personal information to claim the trip, a pop-up message would appear prompting the user to not enter personal information and to delete the email. If interested, users have the have the option to expand the message and read further as to why this is dangerous. Another example could occur in online video games. Often times, pop-up ads will appear promising free coins or upgrades to the game that will transfer the user to a different website. On this website, it will ask users to

download a file containing the upgrades which then will put a virus on the computer or smart device. By using this app when playing online games, the app will recognize these pop-up ads and display a message prompting the user to not enter these websites and why is dangerous. The goal of this APP is to encourage users to practice these habits rather than just hearing about how to stay safe. From my experience, it is better to understand things through experience. It is understandable as well that some are opposite and learn better by reading or listening. For those who prefer to read rather than "do", users will also have the option to read about online safety through a separate document available on the APP. The topics discussed in this document will include:

- Cyberbullying (including tips on what to do if you become a victim)
- Protecting personal information
- Offensive or illegal contact
- Digital reputation

Barriers: The idea for the APP is to be able to recognize dangerous situations on the Internet and display messages to guide users. However, there are some situations that may appear dangerous but are legitimate. For example, if a user receives an email from a teacher who uses improper grammar, has no subject head, and the email server is not familiar with the address, the APP may recognize it as a hazardous email. Another example, involving social media, may occur if someone that the user knows creates an account and asks to follow the user. If this person has just created an account, they most likely will not have many followers, or possibly even a profile picture. These are signs of a suspicious account that users should not accept to follow, but in this case, it would be a legitimate account.

Assessment: To determine if this APP is successful, a survey should be conducted on children and teenagers to see how many participants use this APP for online activity. A recent survey conducted by the Office of Children's eSafety Commissioner showed that children and teens, between the ages of 8 and 17, use social media the most (Office of Children's eSafety Commissioner, 2016). Therefore, when conducting this survey, we will ask children between age 8 and 17 who regularly use the Internet to download this APP for a period of 3 months. If, within these 3 months, some participants forget about the APP and stop using it, it will be concluded that the APP lacks appeal and is not successful. In that case, changes will be made to keep the users interested. If more than 60% of participants actively use the APP for the whole 3 months, it will be concluded that the APP is successful. It is also important to document at the beginning of the survey how many participants already use safe security measures on the Internet. If the APP is successful, there should an increase in how many participants answer "yes". Other important questions to document and assess are "How many participants have ever felt unsafe on the Internet?" and "How much time do you spend on social media in a day?" As mentioned previously, only 33% of households with Internet access are protecting their children by using filtering or blocking software. To know if this APP will be successful, this number should increase significantly.

References

Commissioner, O. o. (2016). Retrieved from https://www.esafety.gov.au/esafety-information

GuardChild. (2019). Protecting Children in the Digital Age. Retrieved from https://www.guardchild.com

SentryPC. (2018). Are Your Children Protected? Retrieved from https://www.sentrypc.com/home/statistics.htm