Taryn Gilbert

Dr. Brian Payne

CYSE 494

June 22, 2019

J.E.T.: A Solution to Educating Children On Internet Safety

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. While researching internet safety for youths, I found that although it may seem that malware attacks and hacking only happens 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. Setting up Parental Controls is a smart way to keep children out of danger, 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. In order to educate children on Internet safety, I have created J.E.T.: a smartphone application that teaches children and teens healthy habits on how to be safe on the Internet. This APP acts as a virtual machine and displays pop-up messages when users enter social media sites, view emails, play online video games, and use video streaming sites. When a user enters vulnerable websites through this APP, pop-up messages will appear which will give advice and tips on what to do and what not to do. If interested, users have the option to expand the message and read further as to why this is dangerous. For those who prefer to read rather than practice these habits hands-on, 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, and digital reputation.

My goal in this paper is to raise awareness about internet safety for youths and resolve the problem by introducing my smart-device application, J.E.T. To achieve this goal, I have organized my paper into five sections. In the first section I provide a literature review about internet safety and explain why it is a problem. This section is divided into 4 sub-sections, cyberbullying, protecting personal information, offensive and violent contact, and digital reputation. In the second section, I explain how the problem and my innovation relate to material that has been covered in classes outside of cybersecurity. Next, I assess my innovation to determine if it will be effective. In the fourth section, I describe the steps needed to take in order to turn J.E.T. into a reality. I end my paper by providing a summary of the next steps needed to continue the process of my innovation.

LITERATURE REVIEW

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). 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). 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)

Cyberbullying. Cyberbullying has been a conflict since the 1990's when personal computers became affordable. In the 90's, cyberbullying mainly occurred in chat rooms and on private messaging sites. Cyberbullying reached its peak in 2010 when it progressed to phone calls, text and instant messaging, and even video clips. Some of the most common cyberbullying behaviors include cyber-stalking, outing, harassment, trolling, and exclusion (Arsenault et al., "Cyberbullying in School"). In March and April of 2007, a random self-report survey was conducted about Internet use and cyberbullying experiences. 1,963 middle school students from 30 schools in one of the largest school districts in the United States completed this survey. From this survey, Justin W. Patchin and Sameer Hinduja found that "students who experienced cyberbullying, both as victim and offender, had significantly lower self-esteem that those who had little or no experience with cyberbullying" ("Cyberbullying and Self-Esteem"). Besides low self-esteem, cyberbullying can also be linked to anxiety,

depression, self-harm, and in extreme cases, suicide. Because cyberbullying can directly affect adolescents at school, some schools have responded by banning cell phones during school hours. Not much information is provided on the internet about how schools address cyberbullying. Upon further research, it has been concluded that "data to guide decisions about the age at which such education should begin, and who would have primary responsibility for teaching this topic are incomplete" (Moreno et al., "Internet Safety Education for Youth"). When students aged 11-16 were surveyed by Peter Smith et al., a majority of cyberbully victims recommended blocking/avoiding messages and telling someone as the best solution to cyberbullying. The same study found that most victims had told nobody about it ("Cyberbullying").

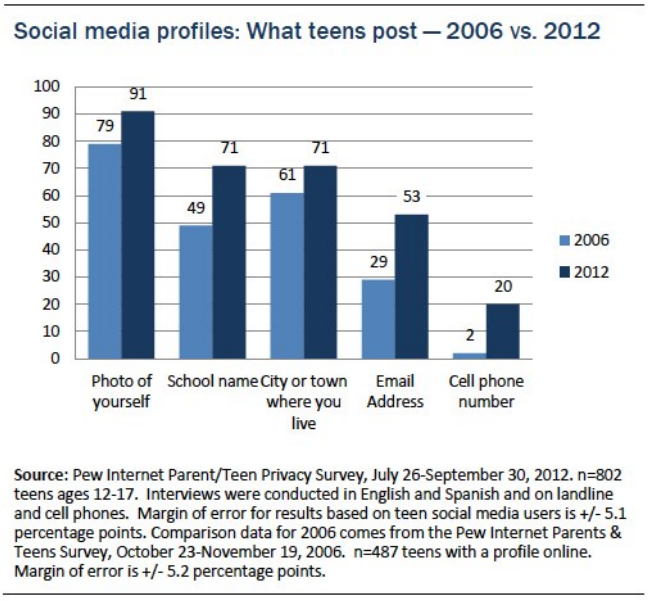
Besides dealing with internalization problems, victims of cyberbullying may also struggle to maintain relationships with others. In a review written by Charisse L. Nixon, the effects of cyberbullying are examined in detailed. Nixon states, "Not surprisingly, targets of cyberbullying reported fewer friendships, more emotional and peer relationship problems, lower school attachment, and more empathy" ("Current Perspectives"). Nixon continues the review by explaining how the effects of cyberbullying can remain, even after the cyberbullying has stopped. "Importantly, the relationship between cybervictimization and adolescents' psychosocial problems remain even after controlling for relational and physical forms of victimization, as well as school-based victimization" (Nixon).

Protecting Personal Information. According to a study conducted by Pew Research Center, "Teens are increasingly sharing personal information on social media sites, a trend that is

likely driven by the evolution of the platforms teens use as well as changing norms around sharing" (Madden et al.). Trends on the internet are generally linked to gender. Cyberbullying, for example, has a higher rate of female victims compared to male victims. When it comes to sharing personal information on the internet, Pew Research Center has found that boys and girls share personal information at the same rate. Instead of gender being a factor, age plays a more significant role. Compared to teens in 2006, who used social media, teens in 2012 share more information on their profiles. Older teens, ages 14-17, compared to younger teens, ages 12-13, share more photos of themselves, their school name, their email, and their cell phone number at a higher rate (see table 1).

Table 1

Social media profiles: What teens post – 2006 vs. 2012



Source: Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. "Teens, Social Media, and Privacy". https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

> "When asked whether [teens] thought Facebook gives anyone else access to the information they share, one middle schooler wrote: 'Anyone who isn't friends with me cannot see anything about my profile except my name and gender. I don't believe that [Facebook] would do anything with my info.' Other high schoolers shared similar sentiments, believing that Facebook would not or should not share their information" (Pew Research Center, "Teens, Social Media, and Privacy").

According to Joiner R, et al., "A previous study found that one-third of adolescents had given their internet password to friends and one-fourth were unaware that content uploaded online cannot be permanently deleted" ("Gender, Internet Identification, and Internet Anxiety").

Besides basic profile information, sharing a user's location has become the norm for teenagers. Over the past few years, social media platforms such as Snapchat, Twitter, Instagram, and Facebook have presented the option of a user being able to share their location. On Facebook, users have the option to "check-in" to a location, notifying their friends of their whereabouts. Instagram and Snapchat offer similar features by allowing users to tag their location on a photo, also allowing followers to see where they are. While some users may feel like it is important to keep their friends updated on their daily activities, sharing your location can be very dangerous. "Some schools have criticized the accuracy of the location-sharing feature, with one warning that it could be used to build up a picture of home addresses, travel routes, schools and workplaces (BBC News). Sharing your location can also pose a risk of strangers having access to your location. Angie Greaves states in an

article, “One of your “friends/contacts” leaves their Facebook account logged in on a publicly shared computer. Someone else gets on that computer and instantly has access to your info since you are the friend of the logged in user” (Greaves).

Offensive or Violent Contact. According to the American Academy of Pediatrics, “American children between 8 and 18 years of age spend an average of 6 hours and 21 minutes each day using entertainment media (television, commercial or self-recorded video, movies, video games, print, radio, recorded music, computers, and the Internet)” (“Media Violence”) Whether positive or negative, mass media has an effect on a child’s behavior, values, and beliefs. According to Sutter Health, “The most widely acknowledged ‘positive’ impact is that video games may help children improve their manual dexterity and computer literacy” (Norcia). The positive impact of video games can be rewarding to a child’s development, but with violent video games becoming more popular, the negative effects play a larger role in a child’s behavior. Recent studies have concluded that violent content in media has been linked to violent behavior, emotions, and decreased empathy in adolescents.

> “Gentile & Anderson (2003) state that playing video games may increase aggressive behavior because violent acts are continually repeated throughout the video game. This method of repetition has long been considered an effective teaching method in reinforcing learning patterns” (Norcia).

The American Psychological Association touched on violence in the media in an article by stating, “A 2010 review by psychologist Craig A. Anderson and others concluded that “the evidence strongly suggests that exposure to violent video games is a causal risk factor for

increased aggressive behavior, aggressive cognition, and aggressive affect and for decreased empathy and prosocial behavior." ("Violence in the Media").

Video games are not the only type of media that can cause violent behavior. In 2017, researchers from Ohio State University conducted an experiment to determine whether violent media plays a role on how children interact with each other. The researchers showed one set of 8-12 year old's a movie with guns in it, and the other set the edited version of the movie with no guns. After the movie, the children went into a play room with nerf guns, Legos, and games. The researchers noticed that the children who watched the movie played more aggressively than the children who watched the movie with no guns. In the playroom, the researchers also placed a real, unloaded gun in a cabinet. "About 83 percent of the kids in the study found the gun, and most of them played with it. Of the kids who found it, 27 percent immediately gave it to the experimenter and the experimenter took it out of the room" (LoBue). The kids who watched the movie with guns pulled the trigger of the fun 2-3 times and held the fun 4-5 times longer than compared to the kids who watched the movie with no guns. While this experiment is very alarming, it is important to conclude that violence plays a large part in the development of a child's actions and behavior.

Digital Reputation. While it is important for children to stay safe on the internet, it is also important to learn what is appropriate to post and maintain a well-managed digital reputation. At a young age, most children and teens do not know that what they post online cannot be deleted, and more people than they realize have access to what they post. In an article posted by Social Digital Mentors, digital reputation is discussed in reference to jobs.

> "An online reputation research commissioned by Microsoft and conducted by Cross-Tab between December 10 and 23, 2009, in France, Germany, the United Kingdom, and the United States, shows that 70% of recruiters would reject candidates based on their online footprint. Some of the reasons mentioned for rejections were the detection of online content connecting the candidates to: alcohol & drugs, bad communication skills and discriminatory content" ("What is Digital Reputation?").

Forbes also makes a great connection about how what we perceive and believe online, represents our digital reputation. Pew Research Center conducted a study and concluded that 91% of people trust what they see and read in search engine results. The Edelman Trust Barometer also reported that 65% of people trust these results more than any other source (Donnelly). Digital reputation is a concept integrated in J.E.T. that I believe could benefit children and teens in their future. To better understand this concept, Internet Society describes digital footprints. "Your digital footprint is all the stuff you leave behind as you use the Internet. Comments on social media, Skype calls, app use and email records- it's part of your online history and can potentially be seen by other people, or tracked in a database" (Society).

> "Your digital footprint is often used to obtain personal info about you, such as demographics, religion, political affiliations or interests. Information could be gathered using cookies, which are small files websites store on your computer after your first visit to track user activity" (Ericksen).

J.E.T. Related to Coursework Outside of Cybersecurity

J.E.T. is a great innovation because it directly correlates with cybersecurity which is not only my major, but a fast-growing field. It is easy to relate the problem to classes I have taken inside of my major, but it can also relate to material outside of my major. In past semesters, I took an interest in criminal justice which led me to take Crime, Society, and the Media and Juvenile Delinquency.

In Crime, Society, and the Media, one of the topics discussed was juveniles. According to my notes from this class, a study of more than 7,500 stories on more than 550 television broadcasts found about 1,700 crime-related stories. About one-third of those stories focused on juveniles as and/or victims. With this alarming rate of juveniles in the media for crime-related stories, it raises a concern as to what causes adolescents to become juveniles. According to James Friedman, a New Jersey Criminal Defense Attorney, "text messages, as well as photos and verbal exchanges from social media, are playing increasingly significant roles in juvenile cases" ("Juvenile Delinquency Cases"). Friedman goes on in the article to explain that it is becoming a practice for prosecutors to check juveniles' phones and social media any time they are under investigation. Although it is common to check social media and cell phones during any investigation, Friedman blames the lack of internet safety on irresponsibility.

> "Juveniles are irresponsible, and that irresponsibility is reflected in their reckless use of social media and cell phones. Kids are being sent to youth facilities and, depending upon the severity of the charges, having their cases

> waived up to adult court, because of the content of their text messages and social media posts" (Friedman)

Rowena E. Mojares et al., also describes how social media relates to juvenile delinquency in a study found in the International Journal of Management Sciences. In this study, 81 high school students, 13 grade school students, 5 out of school youth and 1 college undergraduate responded to a questionnaire to determine which social networking sites were mostly used, to identify which of those sites contributed to the development of delinquency, and to measure counter ill effects of social networking to juvenile delinquency. The results of the study concluded that,

> "It was found that among social networking sites, Facebook is mostly used. As perceived by the respondents, Facebook is the top social networking site that greatly contributes to the development of juvenile delinquency. The gap between the parent and juvenile which social networking greatly widens be filled by building up the communication block with each other" (Mojares et al.).

A child's development is heavily associated with technology as previously mentioned. In a class that I took, titled Juvenile Delinquency, we learned that teens today face social, personal, educational, and financial problems that impede their development such as parental separation and divorce, foster care system, inadequate educational attainment, and coping with the modern world. All of these developmental factors are examples of what causes juvenile delinquency. Because technology plays a role in a child's social, personal, and educational development as

well, it is important for kids to have the best knowledge about the Internet in order to decrease the problems that the youth already face.

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.

TURNING J.E.T. INTO A REALITY

In order to turn J.E.T. into a reality, the first step is to find an investor. When pitching the idea to the investor, it is important to highlight the deference between J.E.T. and similar APPs. When taking a look at APPS that are designed to keep children out of danger on the Internet, there is a theme. Boomerang Parental Control allows kids to browse the Internet with a built-in filter for inappropriate websites. Kidgy monitors your child's activity and also acts a GPS system to keep tabs on your child. Net Nanny is an APP that blocks dangerous websites from children (Educational App Store). (SentryPC)All of these APPS are parental-control oriented. Blocking children from dangerous websites is very important but teaching them why certain websites are dangerous is even more important. That's why J.E.T. was created. To not only teach children and teens about Internet safety, but to implement healthy habits into their daily online routine.

These APPS also have another theme in how they're being promoted. Most ads for these APPS pop up on kids' websites pages. The idea of the APP is to grab the parent's attention to have them implement the APP into their child's lives. So how do we grab parent's attention? According to Pew Research Center, Millennial women (those born from 1981 to 1996) accounted for 82% of U.S. births in 2016. Those same millennials made up 90% of U.S. adults who use at least one social media site as of February 2019. If we can get one parent to review this APP and share it with their kids' friends on Facebook, Snapchat, Twitter, etc., word about how great J.E.T. is would spread very quickly.

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. Because of these barriers, the next step in turning J.E.T. into a reality is to invest in a well-known, educated engineer to ensure that these barriers will be eliminated.

NEXT STEPS

The next step in this innovation process is to re-evaluate the business model canvas. The business model canvas is the most important part to an innovation and it should be double-checked to ensure everything is correct. The next step is to present my idea to an investor. My group is in the process of creating a pitch that can be presented to investors and presenting this pitch the right way is also key in getting my business started. According to a YouTube video posted by Donna Grif, the main points to focus on when presenting a pitch are:

- Focus on the ***pain*** – less than a minute for short form
- Demonstrate the reachable market
- Explain the business model
- Tout the management team
- Explain your metrics

- Motivate the audience
- Why ***you*** and why ***now***?
- Rehearse

After the pitch, the main focus should be how to expand the business. Because schools are so involved with children and the internet, a great place to look to expand the business are schools. If this APP succeeds, upgrades and modifications could be made to make a program that can be integrated into school computers. The goal of this APP is to encourage users to practice these habits rather than just hearing about how to stay safe and practicing these concepts at school could be beneficial to students as well as teachers.

Works Cited

Association, American Psychological. Violence in the Media. 12 November 2013. 6 May 2019.

Donnelly, Tripp. Why Your Digital Reputation Matter and How to Influence It. 7 May 2018. 3 June 2019.

Ericksen, Kristina. Your Digital Footprint. 16 May 2018. 4 May 2019.

Friedman, James S. Juvenile Delinquency Cases, Texting, and Use of Social Media. 23 December 2016. 15 June 2019.

Greaves, Angie. The Dangers of Location Sharing. 13 March 2018. June 6 2019.

LoBue, Vanessa. Violent Media and Aggressive Behavior in Children . 8 January 2018. 22 June 2019.

Madden, Mary, et al. Teens, Social Media, and Privacy. 21 May 2013. 15 June 2019.

Mentors, Social Digital. What is Digital Reputation . 13 January 2019. 15 June 2019.

Mojares, Rowena, et al. Impact of Social Networking to Juvenile Delinquency. 8 November 2015. 19 June 2019.

News, BBC. Schools Issue Snapchat Map Warning. 5 July 2017. 15 June 2019.

Norcia, Andrea. The Impact of Video Games. June 2014. 17 June 2019.

Pediatrics, American Academy of. Media Violence. 8 November 2009. 17 May 2019.

SentryPC. Are Your Children Protected? 6 April 2018. 3 June 2019.

Society, Internet. Your Digital Footprint Matters. 6 November 2018. 12 June 2019.

Store, Educational APP. Best Safe Browsing Apps to Keep Your Kids Safe. 2019. 3 May 2019.