



**THE UNIVERSITY OF  
WESTERN AUSTRALIA**

*Achieve International Excellence*

**School of Computer Science and Software Engineering**

**Research Project**

**Semester 2, 2019**

**Understanding the Effects of Cybersecurity Gamification  
on Female Engagement & Motivation**

**Author: Dina Jaber - 21812873**

**Supervisor: Dr. Jin Hong**

## Abstract

There is a severe lack of gender diversity in the cybersecurity field that needs to be addressed. Cybersecurity gamification has been proposed as a method of encouraging and engaging young females with cybersecurity. This project aims to investigate the effect game-based learning has as a strategy to teach and engage cybersecurity to young adults and to motivate young females to pursue cybersecurity as an educational pathway and future career. This will be done by identifying and understanding gaming trends and the engagement factors that drive people to play games. In addition, the gaps in knowledge regarding cybersecurity topics that young adults have will be identified and targeted. A pre-survey questionnaire will be created and distributed which will be studied and analysed to understand if patterns and differences exist between gender and the following: game genres, gaming elements, and cybersecurity education. The results of the pre-survey will then be used to develop a cybersecurity game to be used as an educational tool. A post-survey will then be conducted and investigated to understand the usefulness of cybersecurity gamification on younger generations.

## Introduction

The number of cybersecurity incidents are increasing rapidly, negatively impacting businesses, governments and individuals daily. According to a report released in 2018 by McAfee, the annual current estimate of cybercrime may now cost the world around 600 billion US dollars. The data was collected from surveys performed in over 50 countries and it is estimated that more than two billion individuals have been subject to theft of personal information [1]. Consequently, the demand for cybersecurity specialists has increased over the years, and it has been predicted that by the year 2022 there will be vacancies for 1.8 million people in the cybersecurity sector [2]. However, it is challenging to recruit cybersecurity specialists, especially females. Previous studies have shown that gender diversity in the work environment has led to a broadening in the range of skills, experiences and perspectives brought to challenges [3]. In addition, increasing diversity drives economic growth as it yields a more competitive workforce leading to better problem solving [4]. Unfortunately, there is a lack of interest from female students to take up computer science subjects such as cybersecurity, leading to severe gender imbalance in the cybersecurity workforce [4].

At school, students are exposed to various forms of technology and taught how to use them. However, the knowledge of the threats that they face while using technology and how to counteract the threats are not acknowledged as part of the curricula [5]. Moreover, human-decision making has been one of the significant factors contributing to security threats. Verizon's annual Data Breach Investigation report identified in a survey of around 80,000 people that "human error, deliberate actions, or insufficient training and awareness" are the key factors instigating security breaches [6]. Students need to be trained with necessary cybersecurity knowledge and skills as this will lead to a decrease in security breaches and hopefully inspire more students to join the cybersecurity workforce. According to Javidi and Sheybani [4], growing cybersecurity personnel is a "multi-year proposition, as it takes years of experience to develop maturity in the requisite knowledge, skills and abilities to perform many of the complex security tasks". This enforces the need to begin educating students during early stages regarding cybersecurity principles so that they have the initial skills and motivation necessary to lead them to prosper in a career in cybersecurity. Cybersecurity education can begin in the classroom in the form of gamification where game design elements such as aesthetics, mechanics and dynamics are used in non-game contexts such as learning [7]. Game-based learning is a multi-faceted field that encapsulates "virtual reality games, web-based games, multi-user virtual environments, massively multiplayer online games, and simulations" [8]. Effective gamification designs can simulate real world problems allowing students to gain an in-depth understanding of how to apply conceptual knowledge that has been learned. Problem solving, logical thinking, productive struggle and cooperation skills can all be learnt in a more playful and engaging manner. Students are provided with the opportunity to experiment and make mistakes in a risk-free setting, actively practicing and learning the correct methods of performing tasks related to the topic of the game [8]. Gamification has the benefit of creating a positive student experience that is enjoyable, supplying constant feedback, and providing both intrinsic and extrinsic motivation for students [9].

Designing an educational cybersecurity game requires an understanding of what gaming elements attract players enough to dedicate time and effort to certain games. Furthermore, it becomes more complicated because female and male audiences have different preferences when it comes to gaming elements. Gender plays a large role when it comes to designing games and research shows that the motivations people have for playing games and that the emotions and play style experienced during games differ when it comes to gender [7]. Evidence exists that women and men tend to favour social interaction in video games differently. In addition, there are several gender differences in terms of games genres. Males tend to prefer playing more physical (sports) and violent (shooting) games whereas females are more inclined towards genres such as puzzle games [10]. As a result of all these differences, gamification techniques need to be carefully considered when designing a game. A balance needs to be found where cybersecurity gamification can engage both males and females. At the same time, the game needs to motivate females to pursue a career in cybersecurity to help remedy the current gender gap.

The application of gamification on cybersecurity education has the potential to increase both student engagement and motivation. In addition, cybersecurity gamification may be able to encourage more females to seek STEM roles as their future profession and minimise the gender gap that is significantly prominent in the cybersecurity workforce.

## Related Work

### Females in STEM and Cybersecurity

Skills in science, technology, engineering and mathematics (STEM) are the innovating force behind economic growth [11]. They provide people with the ability to solve problems, think critically and struggle productively. Industries nowadays are becoming increasingly dependent on technology and as a result the demand for a workforce with skills in STEM has risen rapidly. However, even though there will be around 1.7 million STEM jobs available in the coming years, the STEM workforce continues to be dominated by men [12]. Table 1 shows the statistics of women graduated in post-secondary institutions in the US between 2015 - 2016. The table statistics show that the percentage of women that earned degrees in STEM fields was significantly low with similar numbers being mirrored in Canada and the European Union. In Australia, women in STEM are highly underrepresented, 2016 statistics showed that Australia's STEM workforce was made up of 27% women and the engineering workforce of only 12.4% women [13].

*Table 1 - Percentage of Degrees Earned by Women in Postsecondary Institutions in the United States (2015–2016) [13]*

	<b>Bachelor's</b>	<b>Master's</b>	<b>PhD</b>
<b>Biological and biomedical sciences</b>	59.9%	57.3%	53.0%
<b>Mathematics and statistics</b>	42.5%	41.7%	28.5%
<b>Physical sciences and science technologies</b>	38.8%	37.8%	32.2%
<b>Engineering and engineering technologies</b>	19.7%	25.2%	23.5%
<b>Computer and information sciences and support services</b>	18.7%	30.8%	20.1%
<b>All STEM Fields</b>	35.5%	32.6%	33.7%

The statistics indicate that the gender gap that exists in STEM fields is a worldwide phenomenon. Research suggests that gender diverse companies outperform businesses that do not possess the same levels of diversity [11]. Increasing the participation of women in STEM in Australia by simply 6% could lead to an increase in \$25 billion to Australia's Gross Domestic Product [11].

Of all the STEM fields, the cybersecurity workforce is an area where females are most underrepresented. Information systems have been embedded into our everyday lives and will be entrusted with our national security, privacy, safety and digital identities [14]. Of the cybersecurity specialists currently employed, women comprise of only 11% of the global cybersecurity profession [15]. Addressing the gender imbalance that exists in cybersecurity fields has the potential of fixing the shortage of personnel in cybersecurity. In addition, diversified teams have better performance rates, more innovative solutions and offer different perspectives towards challenges [16]. Studies indicate that women examine problems in a cognitively different manner than men and may lead to creatively better solutions [16]. It is of great importance to gain an understanding as to why women are not entering cybersecurity and other STEM fields so that more diversity can be introduced.

The reasons behind the lack of women in cybersecurity and STEM fields are complicated and have long been studied. One of the outstanding reasons are that prominent adult figures such as parents, teachers and career counsellors communicate across to girls and young women their own gender-biased beliefs and stereotypes regarding the abilities and roles fit for females/males which sets their expectancies of themselves [17]. The idea that STEM fields are better fit for males is translated across to them which creates a barrier that stops females from participating in STEM. In addition, the lack of female role models in STEM fields is another reason why younger females do not embark on or persist with careers in STEM [14].

Motivating females to participate in STEM and cybersecurity roles needs to begin at an early age. The National Center for Women and Information Technology (NCWIT) reported that in the United States only 19% of the adolescent test takers taking AP Computer Science were girls [4]. Even though girls perform similarly to boys when it comes to achievement levels at school and university, they continue to display less positivity and lower confidence in themselves and their abilities when it comes to computer science subjects. The low self-esteem and sense of belonging that females have towards their abilities in these fields at both university and high school level can be solved by exposing them to cybersecurity and engaging them with it during adolescence. According to Jethwani et al. [4] research shows that female teenagers lack awareness regarding the different roles that cybersecurity encompasses and are under the perception that computer science careers are restricted to programming and gaming. Moreover, females are under the impression that cybersecurity is not a collaborative work environment and that it does not have social applications which is what tends to appeal to girls. Females at school need to be exposed to cybersecurity as a field uniquely on its own in a motivating and engaging way. Cybersecurity needs to be demonstrated as the collaborative and creative process that it is, as well as having real world applications that serve society. This can be done by using cybersecurity gamification as a method to appeal to the female population during initial stages at school.

### Cybersecurity Gamification for Education

Cybersecurity is an area of study that lends itself well to gamification [18]. It is traditionally taught to students in classroom environments through reading, watching videos, and practicing at home. However, through game-based learning - cybersecurity knowledge, skills and reaction times can be put to the test in real world simulations, without risking “real-world assets” such as money and data [8].

Herr and Allen [18] stated that playing traditional video games improves spatial reasoning, motor skills, decision-making and reduces stress. The challenges and interactions with players presented in a cybersecurity game have the potential to improve students’ cooperative skills whilst providing them with the necessary knowledge and training required. There is no single target audience when it comes to gaming as Herr and Allen found that games have very diverse demographics with forty percent of gamers being women [18]. With such a large percentage of gamers being female, it would be possible that cybersecurity gamification will not only raise awareness in cybersecurity for young adults, but also motivate more females to enter the industry.

Awojana and Chou [19] describe and evaluate various game-based learning tools developed to educate people in cybersecurity. Table 2 groups the games depending on their category and lists the benefits and limitations of each of the games.

*Table 2 - Existing game-based learning systems in cybersecurity [19]*

Category	Games	Advantages	Disadvantages
<b>Single Player</b>	CyberAware CyberProtect CyberCIEGE PhishGuru	Scalable and fixable.	Players' lose interest overtime as it becomes less challenging.
		User friendly interface.	Result of players' choices are against discrete and algorithmic opponents.
		Stimulates players interest with educational scenarios.	
<b>Multi-player</b>	GenCyber CyberNEXS SecurityCom InCTF	Increase in social interaction using team competitions.	Consume substantial space and bandwidth.
		Increase in engagement levels amongst players.	Time consuming as different individuals/teams need to be consulted.
		Scalable, flexible and interactive.	
		Players learn to think like attackers/defenders and gain skills that can be applied in the real-world.	

The results of the study indicate what game features appealed to participants more successfully. However, analysis in to how these games have differed in terms of gender has not been done. Indication as to whether the games successfully resonated with both males and females remains unclear.

### Differences in Gaming Elements and Engagement between Males and Females

Creating an educational cybersecurity game will raise awareness regarding the criticality of cybersecurity and motivate students to become interested in seeking it out as an education pathway. However, the main goal is to increase diversity within the cybersecurity workforce by influencing more females to become involved. Designing an educational game that will engage both males and females is a difficult task as research has shown that there are differences amongst the game genres that males and females prefer to play and between the elements that captivate them to play games [20]. Even though women and men play video games in approximately equal numbers, stereotypes continue to exist associating video games with only men [21].

With regards to game genres, it has been found that females and males have different preferences. The results of a study performed by Paaßen et al. [21] showed that 85.9% of males played hard-core games (identified in this study as shooters, massive multiplayer games, and real-time strategy games) whereas only 42.7% of the women did. In addition, they stated that shooter games such as *Halo* and *Call of Duty* have identified 27% and 28% of

their gamer population as females respectively. Moreover, *League of Legends* which is a strategy game has a statistic of about 29% of their players being female. Games with manageable challenges, ease of use and long-term relationship building such as *Farmville* and *Candy Crush* are predominantly played by females [21].

Furthermore, an analysis was performed in Belgium that examined genre preferences, playing frequency, the influence of gender and gaming beliefs [22]. The study concluded that:

- The genres males prefer to play are growth (MMORPGs, strategy games), heavy action (shooting and survival horror games) and sports.
- The genres females prefer to play are casual (card and puzzle games).
- No gender differences were found for linear progression genres (platform and adventure games).
- A larger number of high-frequency (hardcore/moderate gamers) male players believe that “gaming is a pastime for boys” than high-frequency female players do.
- More high-frequency male players believe that “boys are better at gaming” than high-frequency female players do.

Most of the data found indicates that a gender difference in preferences does exist when it comes to game genres. In addition, there is a stereotypical belief amongst all genders that males are the better and more-frequent gamers.

Regarding the motivation behind what pushes males and females to play games, it has been found that males are more attracted to achievement and competitive games with elements such as leaderboards and point systems [20]. Female players, however, may be less motivated by these types of games. Another aspect is that male players have a higher level of enjoyment for 3D-rotational games than females do. In terms of the social aspects of gamification, females have been found to perceive the social community within a game and the benefits that accompany them as more valuable features than males [23]. Females who are frequent gamers view games as platforms to socialise with friends and family as well as a chance to meet new people. This indicates that social aspects may be necessary if female players are to be sought after as an audience for a game.

Investigating gender differences in gaming engagement revealed that there are important considerations that need to be taken when designing an educational cybersecurity game. Considering the area of gender differences in cybersecurity gamification has not been thoroughly assessed, this project could help shed some understanding on the topic.



## Methodology

Understanding the factors that influence players to engage with a game and what elements trigger participation and enjoyment requires thorough research to be conducted. A pre-survey questionnaire was generated and distributed to the public with the goal of obtaining data that would aid in the design of an educational cybersecurity game. Once the game is created, it will be used as a learning experience and tested by participants. The final step is to understand whether gamification did indeed have a positive impact in motivating students towards cybersecurity and particularly if females actively engaged in the game. This will be done by conducting a post-survey questionnaire and analysing the responses the participants will have with the game.

### Pre-Survey Questionnaire

The pre-survey will be distributed on online websites/forums/communities (e.g. gaming forums), by word of mouth and on social media via *surveyplanet* which is an online survey tool. Table 3 shows the different sections created in the questionnaire.

*Table 3 - Categories in the pre-survey questionnaire*

Section topic	Section description
<b>Demographic questions</b>	Asks generic questions (age, gender and ethnicity).
<b>Gaming background</b>	Targets the participants gaming background such as previous games played, number of hours played and preferred gaming platforms. This section will help develop an understanding as to whether there are differences between gender preferences regarding these aspects.
<b>Gaming engagement factors</b>	Analyses what features influence and engross people to play games. Investigating this section of the pre-survey will generate a clearer understanding of what engagement elements need to be integrated into a game to motivate males and females to play.
<b>Cybersecurity education</b>	Examines the level of understanding the participants have on cybersecurity topics. The data gathered from this section will be used to understand what topics need to be targeted when developing a cybersecurity educational game.
<b>Game-play attributes</b>	Appraises the main game features that trigger participants sense of excitement when playing games. This section will highlight if there are any differences between game feature preferences and gender.

The questionnaire contains multiple forms of questions and feedback methods. Table 4 illustrates the questions asked as well as options for the statistical methods that could be used to analyse the data.

*Table 4 - Pre-survey questionnaire methods, examples and data analysis methods*

<b>Question/feedback method</b>	<b>Example</b>	<b>Analysis method</b>
<b>Nominal/Category type questions</b>	Gender, ethnicity	Chi-Square test [24]
<b>Ordinal questions</b>	Five-point Likert scale questions from 'strongly disagree' to 'strongly agree' e.g. Do you enjoy learning through educational games?	Mann-Whitney U-test [24]
<b>Ordinal scale questions (ranking)</b>	Rank the following in terms of how you prefer to play a game: Multiplayer/Single Player/Both	Mann-Whitney U-test [24]
<b>Interval questions</b>	Age (years)	t-test [24]
<b>Continuous questions</b>	How many hours do you play per day on average?	Measures of central tendency (mean, median & mode) and the distribution of the responses (range & standard deviation) [25]
<b>Multiple choice questions</b>	What top 3 reasons motivate you to play your favourite game? E.g. Competition/To gain points/To achieve something difficult...	ANOVA [26]

Once the pre-survey data has been collected, the interactions and differences between gender and the questions asked will be analysed. The data will be examined to determine whether there are any trends or themes such as common responses to the questions asked (e.g. game genres). The statistical analysis performed on the data will also explain whether the survey data obtained is meaningful. Once the pre-survey data has been analysed, game design and development will begin.

### **Game Design and Development**

The pre-survey questionnaire will determine what kind of cybersecurity game will be created, the elements it will incorporate and how it will be developed. Possibilities for the engines, tools and platforms that could be used to code and develop the game include Unity, Buildbox and GameMaker: Studio. The results from the pre-survey will shed light on factors such as the most popular gaming platforms used by the participants and preferred gaming visual elements which will be deciding factors in the game engine utilised. The game design stage will include deciding on the game theme and genre, the type of activities that the game will consist of, the game sequences the players will go through, the characters and storylines that will be integrated and the components the game will include such as the tools needed to achieve a goal in the game. In addition, the outcome of the survey will illustrate which

cybersecurity concepts need to be addressed. After the game has been developed, it will be tested by participants who will then answer a post-survey questionnaire regarding the game.

### Post-Survey Questionnaire

The goal behind the post-survey questionnaire will be to understand whether the cybersecurity game created was a successful learning tool at developing the participants knowledge regarding cybersecurity concepts in an engaging manner and whether the female participants felt actively inspired and motivated by the game. This will be done by collecting post-game feedback from the participants. Table 5 illustrates the aspects that the post-survey questionnaire will evaluate as well as example statements that could be asked.

*Table 5 - Post-survey categories and example statements that will be asked*

<b>Post-survey aspect</b>	<b>Example of five-point Likert scale statements ('strongly disagree' to 'strongly agree')</b>
<b>How the participants feel about the gameplay features used - e.g. game content, length, quality and enjoyment level.</b>	The cybersecurity game was enjoyable.
<b>The game's educational value - the level of understanding the participants gained from the game regarding cybersecurity concepts.</b>	The cybersecurity game helped increase my knowledge in phishing security.
<b>The level of motivation, engagement and productivity the participants experienced playing the game.</b>	Gamification is a engaging and productive method of teaching cybersecurity.

The post-survey results will be analysed in an in-depth manner using statistical methods like the pre-survey data and then compared. The results of the comparison will determine whether the cybersecurity game created satisfied the motivations of the project which are:

- To raise knowledge and awareness regarding cybersecurity for young adults.
- To inspire students to enter the cybersecurity field at an early age.
- To teach the younger generations cybersecurity topics in a more innovative and fun manner using gamification.
- To engage females with the game and encourage them to pursue cybersecurity.

## References

- [1] Lewis, J. (2018). *Economic Impact of Cybercrime— No Slowing Down*. Retrieved from <https://www.csis.org/analysis/economic-impact-cybercrime> [Accessed 10 Aug. 2019].
- [2] Jin, G., Tu, M., Kim, T., Heffron, J. and White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning*, 12(1), pp.150-158. doi: <https://doi.org/10.11591/edulearn.v12i1.7736>
- [3] Grimson, J., Grimson, W. (2019). Eliminating Gender Inequality in Engineering, Industry, and Academia. In: Christensen S., Delahousse B., Didier C., Meganck M., Murphy M. (eds) *The Engineering-Business Nexus. Philosophy of Engineering and Technology*, 32, pp 315-339. doi: [https://doi.org/10.1007/978-3-319-99636-3\\_15](https://doi.org/10.1007/978-3-319-99636-3_15)
- [4] Jethwani, M., Mermon, N., Seo, W. and Richer, A. (2017). I Can Actually Be a Super Sleuth”: Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research*, 55(1), pp. 3–25. doi: <https://doi.org/10.1177/0735633116651971>
- [5] Sheybani, E. and Javidi, G. (2018, October). *K-12 Cybersecurity Education, Research, and Outreach*. Paper presented at the 2018 IEEE Frontiers in Education Conference. doi: 10.1109/FIE.2018.8659021
- [6] Leune, K. and Petrilli, S. “Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education,” in *Proc. of the 18th Annual Conference on Information Technology Education*, 2017, pp 48-52, doi: 10.1145/3125659.3125686
- [7] Pedro, L., Lopes, A., Prates, B., Vassileva, J. and Isotani, S. (2015, April). “Does gamification work for boys and girls? An exploratory study with a virtual learning environment,” in *Proc. of the 30th Annual ACM Symposium on Applied Computing*, pp 214-219, doi: 10.1145/2695664.2695752
- [8] Schreuders, Z. and Butterfield, E, Gamification for teaching and learning computer security in higher education. Presented at 2016 USENIX Workshop on Advances in Security Education. [Online]. Available: <https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders>
- [9] Jin, G., Tu, M., Kim, T., Heffron, J. and White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning*, 12(1), pp. 150-158. doi: 10.11591/edulearn.v12i1.7736
- [10] Poels, Y., Annema, J., Verstraete, M., Zaman, B. and Grooff, D. (2011). Are you a gamer? A qualitative study concerning the parameters used to categorize casual and hardcore gamers. Presented at The IADIS International Conference Game and Entertainment Technologies 2011. [Online]. Available: <https://core.ac.uk/download/pdf/34543728.pdf>
- [11] Australian Government. Department of Industry, Innovation and Science. (2019). *Advancing Women in STEM*. Retrieved from <https://www.industry.gov.au/data-and-publications/advancing-women-in-stem>
- [12] Shein, E. (2018). Broadening the path for women in STEM. *Communications of the ACM*, 61(8), pp.19-21. doi: <https://doi.org/10.1145/3231170>

- [13] "Catalyst, Quick Take: Women in Science, Technology, Engineering, and Mathematics (STEM)." Catalyst.org. <https://www.catalyst.org/research/women-in-science-technology-engineering-and-mathematics-stem/> (Accessed Aug. 10, 2019).
- [14] Javidi, G. and Sheybani, E. (2019). Transforming Cybersecurity Education through Consulting. *Systemics, Cybernetics and Informatics*, 17(1), pp 157-168.
- [15] Center for Cyber Safety and Education (2017). *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*. Retrieved from <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf>
- [16] Kembley Kay Lingelbach. (2018). *Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field*. (Doctoral dissertation). Retrieved from NSUWorks, College of Engineering and Computing. (1056) [https://nsuworks.nova.edu/gscis\\_etd/1056](https://nsuworks.nova.edu/gscis_etd/1056).
- [17] Burch, A., & Wiseman, R. Curiosity, courage and camouflage: Revealing the gaming habits of teen girls. (2015). Accessed: Aug 13, 2019. [Online Video]. Available: <http://www.gdcvault.com/play/1021899/Curiosity-Courage-and-Camouflage-Revealing>.
- [18] Herr, C. and Allen, D. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors," in *Proc. of the 2015 ACM SIGMIS Conference on Computers and People Research*. pp.23-29, doi: 10.1145/2751957.2751958
- [19] Awojana, T., & Chou, T. (2019). Overview of Learning Cybersecurity Through Game Based Systems. Presented at 2019 CIEC, New Orleans, LA. [Online]. Available: <https://peer.asee.org/31521>
- [20] Codish, D. and Ravid, G. (2017). "Gender Moderation in Gamification: Does One Size Fit All?," in *The Hawaii International Conference on System Sciences 2017*, doi:10.24251/hicss.2017.244
- [21] Paaßen, B., Stratemeyer, M. and Morgenroth, T. (2017). What is a True Gamer? The Male Gamer Stereotype and the Marginalization of Women in Video Game Culture. *Sex Roles*, 76(7-8), pp.421–435. doi: <http://dx.doi.org/10.1007/s11199-016-0678-y>
- [22] Vermeulen, L. & Van Looy, J. (2016) "I Play So I Am?" A Gender Study into Stereotype Perception and Genre Choice of Digital Game Players, *Journal of Broadcasting & Electronic Media*, 60(2), 286-304, doi: 10.1080/08838151.2016.1164169
- [23] Koivisto, J. and Hamari, J. (2014). Demographic differences in perceived benefits from gamification. *Elsevier*, 35, pp.179-188. doi: <https://doi.org/10.1016/j.chb.2014.03.007>
- [24] McCrum-Gardner, E. Which is the correct statistical test to use?, *Elsevier* 46, 1 (2008), pp. 38-41. doi: <https://doi.org/10.1016/j.bjoms.2007.09.002>
- [25] Southampton Education School, Analysing Questionnaires. (Aug. 12, 2012). Accessed Aug. 20, 2019. [Online Video]. Available: <https://www.youtube.com/watch?v=c5CIF8RIGb4>
- [26] Motulsky, H. (2012). "Choosing a statistical test." Graphpad. <https://www.graphpad.com/support/faqid/1790/> (Accessed Aug. 10, 2019)

## Timeline

