# Project Plan

## A 3D Game to Raise Teenagers' Awareness on Cybersecurity

Bin Ho Ching (3035370375)
Cheng Hong Yin (3035374151)

# Table of Contents

## Introduction

Internet is a crucial part of the world nowadays. There are 4.39 billion uses in January 2019 [1], which is more than half of the world population. Internet allows people to communicate with others, shop online, find resources, entertain, and do many other things. Although it is convenient and useful, it brings risks. People may be aware of some large scale incidents including leakage of clients' data of Faster Payment System, Cathay Pacific or TransUnion [2]. Ransomware attacks like WannaCry had been reported widely [3]. However, they seldom notice those small scale or personal data breach. To enjoy the advantages of the Internet with safety, they should learn more about cybersecurity. The project aims at raising teenagers' awareness of cybersecurity. A 2018 survey stated that over 80% of teenagers play video games [4]. It is believed that video game is a good channel to educate teenagers as learning can be achieved while playing.

The following of the project plan would first state the current situation regarding cybersecurity. Next, it would discuss the main message we would like to include in the game. Then, it would suggest a way to explain cybersecurity in the game for easy understanding. Finally, it would propose a preliminary project schedule.

## Background

While people use the Internet frequently, many may not pay attention to online safety. More than one-fourth of US adults use the same password for all of their accounts [5]. Half of Internet users will click on a link from an unknown sender [5]. Majority of companies do not store clients' data safely and not likely to respond to cyber attacks correctly [5]. Many attacks use services or files that people use frequently such as emails, mobile applications and Microsoft Office format files [5]. Without the proper knowledge and awareness, people could easily fall into these traps or even have no idea that they have been attacked. The consequences may be significant and everyone should take great care about them.

## Objectives

Most of cyberattacks need users to take action before they can successfully obtain information. It is hoped that this game can raise players' awareness on these kinds of attacked and take precautions to avoid falling into those traps.

## Target Audience

Although everyone should learn about cybersecurity, adults are likely to have much knowledge than teenagers due to job training or experience. On the other hand, while more than 90% of teenagers over 13 years old have access to the internet [6], they may not not know how to use it safely. Therefore, the target audiences are teenagers.

## Scope of the work

Cybersecurity is a wide topic. There are different types of attacks targeting specific person, general public, companies, governments and other kinds of target. There are measures to provide protection, prevention or avoidance. This project aims to help teenagers to use the Internet safely. Therefore, the focus would be attacks on specific person or public, and measures applicable by individuals. Others attacks and measures may still be included but may be merely references for those interested.

## Methodology

The game would be developed using Unity for PC platform.

To help teenagers understanding concept regarding cybersecurity, we propose to simulate cyberattacks using real world' examples. For example, hacking others' computers is similar to breaking into others' houses. They have similar purposes but using different means and looking for different things to achieve the purposes. By comparing to more well-known concepts, it is believed that teenagers can understand cybersecurity easily.

The trend of game development is moving towards VR and AR. To attract more teenagers, the game would be developed using VR or AR technology if feasible and suitable.

## Schedule

| | |
|---|---|
| 29 September 2019 | Project plan<br>Project web page |
| October 2019 | Game design (mechanic, story, game flow, etc.) |
| Early to mid November 2019 | Find assets and consider the necessity of making assets on our own |
| Mid November 2019 to December 2019 | Implement UI system and basic mechanic |
| January 2020 to March 2020 | Implement game flow and subsystem |
| 2 February 2020 | Preliminary implementation<br>Interim report |
| April 2020 | Bug fixing, Fine tuning, UAT, any ad hoc work |
| 19 April 2020 | Finalized implementation<br>Final report |

## Reference

1. S. Kemp, “Digital 2019: Global Digital Overview,” DataReportal, 30-Jan-2019. [Online]. Available: https://datareportal.com/reports/digital-2019-global-digital-overview. [Accessed: 19-Sep-2019].

2. M. Ma, “Cyber security you wouldn't credit,” The Standard, 30-Nov-2018. [Online]. Available: http://www.thestandard.com.hk/sections-news_print.php?id=202787. [Accessed: 19-Sep-2019].

3. J. Fruhlinger, “The 6 biggest ransomware attacks of the last 5 years,” CSO Online, 05-Apr-2019. [Online]. Available: https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html. [Accessed: 22-Sep-2019].

4. M. Anderson and J. Jiang, “Teens, Social Media & Technology 2018,” Pew Research Center, 30-Nov-2018. [Online]. Available: https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/. [Accessed: 19-Sep-2019].

5. Hosting Tribunal, “Cybersecurity Statistics that Will Help You Stay Safe in 2019.,” Hosting Tribunal, 19-Aug-2019. [Online]. Available: https://hostingtribunal.com/blog/cybersecurity-statistics/. [Accessed: 19-Sep-2019].

6. M. Anderson, “How parents feel about – and manage – their teens' online behavior and screen time,” Pew Research Center, 22-Mar-2019. [Online]. Available: https://www.pewresearch.org/fact-tank/2019/03/22/how-parents-feel-

about-and-manage-their-teens-online-behavior-and-screen-time/. [Accessed: 19-Sep-2019].