

University of Plymouth

School of computing, Electronics and
mathematics

COMP3000
FINAL STAGE COMPUTING PROJECT
2020/2021

BSc (Hons) Computer and Information
Security

Lee Cadman
10670374

Using software to educate user's in cyber security and
to help reduce security risks.

Acknowledgements

I would like to thank my project supervisor, Hafizul Asad for his continuous open support and guidance throughout the whole project.

Abstract

This report explains my software development project. The main aim was to create an educational android mobile application to educate users in cyber security thus increase their cyber security awareness and possibly reducing future cyber security risks. A small experiment will also be taking place where I will put my mobile application to use.

The report will be separated into sections explaining each aspect of my project from start to finish in detail this will include project background, project aims and objectives, project management, methods of approach, legal and social issues, application development, experiments and results. This report will end with project reflection and conclusion.

Table of contents

Acknowledgement	Page 2
Abstract	Page 2
Table of contents	Page 3
Background	Page 4
Motivation	Page 4
Project Aims	Page 4
Project Objectives	Page 4
Methods of approach	Page 5-13
Legal, Social, Ethical and Professional Issues	Page 13
Project Development..	Page 14-30
Experiments, user results and findings.	Page 30-32
End of project reflection.	Page 33-34
Conclusion.	Page 34
References	Page 35-36

Background

In the advancing world of technology there exists cyber-crime, cyber-crime which forces organisations and businesses around the world to spend time and money to try and protect themselves from malicious cyber-attacks, cyber-attacks which can impact them negatively causing damage and being very costly if the attacks are successful. It is stated in the Accenture cost of cybercrime report that the average cost for companies from cybercrime incidents has increased by 72% and the average number of security breaches by 67% in the years 2014-2019 (The cost of cybercrime, 2019). It is also predicted that \$6 trillion USD cybercrime damages will occur globally in 2021 (Morgan, 2020). This is a huge problem in the world of technology and businesses big or small but what can be done to help this issue?

Human error has a huge part to play in why cybercriminals continue to be successful with committing their crimes. In 2019 90% of the UK data breaches were due to human error (Hill, 2020). Examples of human error can be things such as having a weak passwords that can be comprised easily or upholding bad cyber security practices due to the lack of education or training. Cyber criminals will use different types of attacks knowing that some individuals have lack of security knowledge allowing them to pull off their attacks on the unsuspecting individuals, the most common attacks being malware, phishing, hacking and distributed denial of service attacks (DDOS) (Cyber crime, n.d.).

Since human error plays such a big role in why cyber criminals are successful a good start to combating the cyber criminals and reduce the damage, cost and opportunities would be to educate those who do not have the cyber security knowledge or good security practices. Educating and training individuals will reduce the number of vulnerable targets cyber criminals have which could reduce the overall impact of yearly cybercrime. (Ahola, n.d.)

Motivation

Human error plays a big part in cybersecurity incidents as it can lead to security risks unintentionally and compromise the individual or others around them. By creating this mobile application that includes an educational quiz, strong password generator and password strength checker I am hoping it can help make users more security savvy to help reduce those security risks from human error/lack of cyber security awareness and also improve upon their personal security by including features such as a strong password generator and password strength checker.

Project Aims

The project aim is developing an android mobile application that educates user's in cyber security risks and good cyber security practices to potentially reduce security risks for that individual and improving their personal security.

I aim to produce:

- a) An android mobile application that contains the following features :

- Strong password generator – Generates a strong password for the user with the press of a button.
 - Educational Quiz – Multiple choice quiz.
 - Password strength checker – Allows the users to check the strength of an entered password.
- b) Results from a small experiment involving an aspect of my application.
- c) Final project report that includes all aspects of my project from beginning to end.

Project Objectives

Minimum viable product

The minimum viable product is an android mobile application that has :

- a) A Strong password generator.
- b) A password strength checker.
- c) A educational quiz.

Potential future features

Potential future features could include :

- a) Different types of educational quizzes.
- b) Extra features that improve upon personal security such as a file encryption/decryption feature.

System requirements

For the application to be held to a good standard, user friendly and achieve sufficient functionality a set of minimum requirements were set out.

- a) Clear and concise application interface/design.
- b) Easily navigable.
- c) Fully functional quiz.
- d) Fully functional strong password generator.
- e) Fully functional password strength checker.

Methods of approach

Project management

Sprints

Due to project requirements Microsoft 365 planner was said to be the tool to be used to conduct sprints on but shortly after, in a project lecture it was said we could also use other methods if we wanted to. I chose to use Microsoft word to conduct my sprints in created tables as It was my more

preferable option for conducting sprints. Due to unforeseen circumstances I changed my sprints to monthly periods to give myself more time and breathing space. Sprint templates below :

Backlog Template:

Task ID	Task Name	Notes

Sprint Template:

Date: DDth MMM YYYY – DDth MMM YYYY

Task ID	Task Name	Details	Complete

Sprint 1

Date: 01/11/2020 – 01/12/2020

Task ID	Task Name	Details	Complete
0	Create github repository and invite project supervisor	Github created and supervisor invited as collaborator	Yes
1	Document project aim and initiation	Project aim and introduction were documented.	Yes
2	Create storyboard for application	Storyboard was created.	Yes
3	Choose programming language for application	The programming language java was chosen to use for my application	Yes
4	Choose integrated development environment (IDE)	Android studio was the IDE chosen to build my application.	Yes
5	Project General Research	On going	No
6	Create Risk analysis	Risk analysis created using word	Yes
7	Create UML diagrams for application	UML diagrams created	Yes

Backlog

Task ID	Task Name	Notes
5	Project Research	On going

Sprint 2

Date 01/01/2021 - 01/02/2021

Task ID	Task Name	Details	Complete
5	Project General Research	Research completed	Yes
6	Quiz questions and answers research and documentation	Documented all of the quiz questions and	Yes

		answers I will be using for the quiz part of my application	
7	Create main menu layout (XML) in android studio	Layout created. Images, buttons and text all added.	Yes
8	Create password strength checker layout (XML) in android studio	Layout created. Images, buttons and text all added.	Yes
9	Create strong password generator layout (XML) in android studio	Layout created. Images, buttons and text all added.	Yes
10	Create quiz help layout (XML) in android studio	Layout created	Yes
11	Create password strength checker help layout (XML) in android studio	Layout created	Yes

Sprint 3

Date 01/02/2021 - 01/03/2021

Task ID	Task Name	Details	Complete
12	Create strong password generator class	Strong password generator class created.	Yes
12.1	Create Generate String method and create button with set on click listener calling upon it.	Method and button created. Generates a random strong password from the chosen string of characters.	Yes
12.2	Create text view	Text view created and string appended.	Yes
12.3	Create hide or show password button with set on checked change listener.	Hide or show password check box has been created with needed logic.	Yes
12.4	Create copy to clipboard function.	Copy to clipboard function created. Will copy the generated password to the android clipboard once pressed.	Yes
13	Create project final report skeleton document.	Project final report document created.	Yes
14	Complete project document	Started adding towards the project document	No

Backlog

Task ID	Task Name	Notes
14	Complete project document	On going

Sprint 4

Date 01/03/2021 - 01/04/2021

Task ID	Task Name	Details	Complete
14	Complete project document	Progress on going	No
15	Create project showcase poster	Poster created	Yes
15.1	Create project showcase thumbnail	Thumbnail created	Yes
16	Create password strength checker class	Password strength checker class created	Yes
16.1	Add button with set onclick listener to open the help class.	Button created with logic	Yes
16.2	Create password validator function.	Password validator function created. When the user enters certain characters that meet the logical requirements set, the text colour will change to green and a tick will appear.	Yes
16.3	Create padlock function	When the user enters certain characters that meet the logical requirements set, a padlock will appear indicating the strength of the password	Yes
16.4	Add text to password strength help class	Text added the class that will help the user with this part of the application	Yes

Backlog

Task ID	Task Name	Notes
14	Complete project document	On going

Sprint 5

Date 01/4/2021 - 01/06/2021

Task ID	Task Name	Details	Complete
14	Complete project document	Final project report document completed	Yes
17	Create questions class	Created a class for the questions and answers.	Yes
17.1	Add question list	Question list string array created and questions added	Yes
17.2	Add Questions choices	Question choices string array created and choices added	Yes
17.3	Add correct answers	Correct answers string array created and answers added	Yes
17.4			Yes
18	Create quiz class	Quiz class created.	Yes
18.1	Create buttons with set onclick listener for quiz choices	Buttons created with logic	Yes

18.2	Create update questions and choices function	Function created. Will set the text with the next updated question and choice from the questions class.	Yes
18.3	Create game over function	Game over function created. This function when called will pop up on the users screen and display dialogue and the options to start a new game or go to the main menu..	Yes
18.4	Create update score function	Update score function created. Will update the score if users chooses correctly.	Yes
19	Create quiz help class	Quiz help class created. Class will contain information to help the user if needed.	Yes
19.1	Create scrollable text view	Scrollable text view added. Users will be able to scroll through the text.	Yes
19.2	Add knowledge gained during research to the text view.	Information was added as a string and will aid the user if they need help with learning about the topics and choosing the correct choices	Yes
20	Usability testing forms created	Usability testing forms created for testing feedback	Yes
21	Application experiment participants selected and informed	Following plymouth University ethical guidelines. Close friends and family who are over 18 and non-vulnerable were selected.	Yes
21.1	Record results and reflect in the project document	Results recorded and added to document	Yes
22	Usability testing forms created	Usability testing forms created for testing feedback	Yes
23	Create video explaining the project	5 minute video created and uploaded to youtube	Yes
24	Create presentation for project viva	Presentation created	Yes

Risk analysis plan and review

I used risk analysis to identify possible issues that could arise during the project. I set up back up plans to undertake if the issues did occur. Having measures in place to deal with any problems will help the project run more smoothly as I would not have to decide what to do once it happens as a plan will already be in place.

Most of the risks listed thankfully did not occur. There were a couple that did and this was due to the global pandemic that was on going, cases got more severe so the university had to stay completely online for most of the academic year. Something I did not plan for was the mental health effects of a

global pandemic which included a lengthy lockdown in combination with university work, I wasn't expecting to be so effected by it and due to this I changed how my project sprints were done to give myself more breathing space and to try help with the current situation.

Individual Scores

1 Very Low

2 Low

3 Medium

4 High

5 Very High

Overall Scores

1 - 5 Very Low

6 – 10 Low

11 – 15 Medium

16 – 20 High

21 – 25 Very High

Number	Risk	Description	Impact score	Likelihood score	Overall Score	Mitigation
1	Loss of files	Files could be lost due to faulty or broken hardware. Project could be delayed or not able to be completed.	5	2	10	Make sure I routinely back up the files using a combination of cloud storage and hardware.
2	Plymouth University campus is closed temporarily due to coronavirus	As we are currently in a pandemic due to coronavirus the university campus could close temporarily in a lockdown. This would restrict access to using lab equipment.	1	4	4	Make sure all software needed for the project is installed on personal computer and virtual machine at home.
3	Plymouth University campus is closed permanently due to coronavirus	University could close for the foreseeable future due to coronavirus. This means I would only be able to use my own computer/hardware as the lab would not be accessible.	1	4	4	Make sure all software needed for the project is installed on personal computer and virtual machine at home.
4	Project deadline not being met	The project deadline may not be met due to numerous problems that could occur or poor planning	3	2	6	Create sprints in Microsoft word to keep organised to ensure individual project deadlines are being met.
5	Sprints not being completed/Incorrect assumptions about time required to	Not completing sprints on time multiple times could create a big backlog causing stress and possibly	4	2	6	Make sure project has been planned well and be realistic with my own ability.

	complete tasks within sprints.	delaying project completion.				
6	Home Internet going down	Internet at home could become unavailable which stop work being done on the project from home.	5	2	10	Go to the university (if open) to use lab machines if internet is down for a long period of time/days. Create a hotspot on my mobile so my computer can use my phones data for the internet.
7	Zoom going down	Zoom could become unavailable which would stop weekly video contact with project supervisor.	3	1	3	Use emails to keep in contact with project supervisor or possibly find another platform for video calls.
8	Loss of code/configuration	Loss of code/configuration could delay progress with creating the app	4	2	8	Code will be committed to github.
9	Difficulty using the software/language required	If I am struggling to use the software or language required to create my app this could lead to failure of completing the project.	5	2	10	When planning the project the software and language chosen will be something I am familiar/more experienced with.
10	Catching covid-19	Due to the current global pandemic there is the possibility of catching the virus covid-19. This could leave my unable to do work for a period of time.	5	4	20	Keep to the government guidelines to lower chances of catching the virus. Ensure plans consider this possibility.
11	Inadequately defined requirements	Requirements continually changing throughout the project could lead to design errors due to the original planning not taking them into account.	4	1	4	Make sure during planning, requirements are clearly laid out and project aims are well thought through.
12	Home computer system hardware becoming faulty	The computer system I am using at home becomes unusable due to faulty hardware	5	1	5	Have funds in place to replace the faulty hardware

Tools Used

There were a variety of different tools used in this project to conduct project management, communicate with others, documentation, project design and development. Each tool used will be discussed below.

Android Studio – Android studio is a popular integrated development environment (IDE) and is used for developing android apps. One of the reasons I chose android studio was because it has a wide range of features that give me the best environment for developing an android app at the highest quality. I was also set on using java programming language for developing my mobile app because

that is the language I am most familiar with and it is the official language of android studio. One of the useful features I made use of during the design process was the android studio layout editor, this allowed me to build my mobile interface for the application more efficiently. Instead of writing the layout XML by hand the layout editor allowed me to build layouts by dragging UI elements into the visual design editor and preview what the layout would like look like on mobile devices.

Microsoft word - Microsoft word is a word processing program which allows you to create a document to type text into and save when you are finished, it has a various set of tools which aid you with typing and crating the document. I used this for documenting my research and completing sprints.

Github - Github is a git repository hosting service and provides the web based graphical interface of the command line tool git. I used Github to store the documentation and code for the mobile application I was developing. Github is useful for keeping a backup of all project related files in case something went wrong with the computer I was using to store everything on. If a file that was stored locally on my computer got deleted or was corrupted, I could download the latest committed copy from the git repository.

Google forms - Google forms is an application that allows you to create your own personalized survey and allows you to share with others to fill out. I used this for my usability testing to create a survey and get feedback from others as they were testing my mobile application. Feedback from users is extremely important before rolling out a final application as it gives you a chance to make any changes based on useful feedback or fix any bugs a user may have discovered during testing.

Microsoft Outlook – This is an application that is used to send and receive emails and allows management of emails. I used this to communicate with the project supervisor.

Zoom - Zoom is a cloud-based video conferencing application that allows video or audio communications between multiple users. It has features such as screen sharing and screen annotation. Due to the global pandemic and the university being online there were no face to face meetings so zoom was used to join project meetings hosted by the project supervisor to discuss the project and ask for any advice if needed.

Lucid charts – Lucid chart is a online UML diagram tool that allows the creation of UML diagrams. I used this to create UML charts for my mobile application.

One drive – One drive allows users to store and share files on the cloud. You can have a personal private storage area or a shared area where multiple users have access to and can all view, edit, delete files within that area. As well as using github I used one drive as a resource to back up documentation which gave me that extra security to make sure documents will not get lost or corrupted.

Mindmup - Mindmup is an online web application that allows the creation of mind maps. I used a mind map to brainstorm ideas for my project.

OBS - OBS is a piece of software that is used for recording, sharing and manging videos. This will be used to record a video of my application.

Legal, Social, Ethical and professional issues

Data protection act 2018

The Data protection act 2018 is the UK implementation of the EU's GDPR legislation, it is in place to control how people's personal information is used by organizations, businesses and the government and provides strict guidance for them to follow. Having this law in place will ensure data is used fairly, transparently and lawfully whilst making sure the data is protected against unauthorized access, processing, loss, destruction or damage. The data protection act also gives people the right to find out what information is stored about them by organizations or the government. This allows people access to their personal data which then can be can be chosen to be erased, stop or restrict the processing of their data, have any data that is incorrect updated or they can choose to reuse their data for different services. (Data protection, n.d.)

My application does not have the functionality to save or store users data, so I can ensure I am not breaching the data protection act 2018 guidelines. If future changes of this application did store user's data then the data protection act 2018 guidelines would have to be followed.

Copyright

All images used in the development of this project are not in violation of licensing or copyright laws. I made sure to use royalty free images throughout this project to avoid any ethical issues with copy licensing and copyright laws.

Ethical, professional and social issues

This project is unlikely to cause any ethical, professional or social issues. This project has been approved to be tested and research conducted as long as guidelines are met under the university of Plymouths ethics policy. Close friends and family who are over 18 and not vulnerable are able to take part in my ethical project.

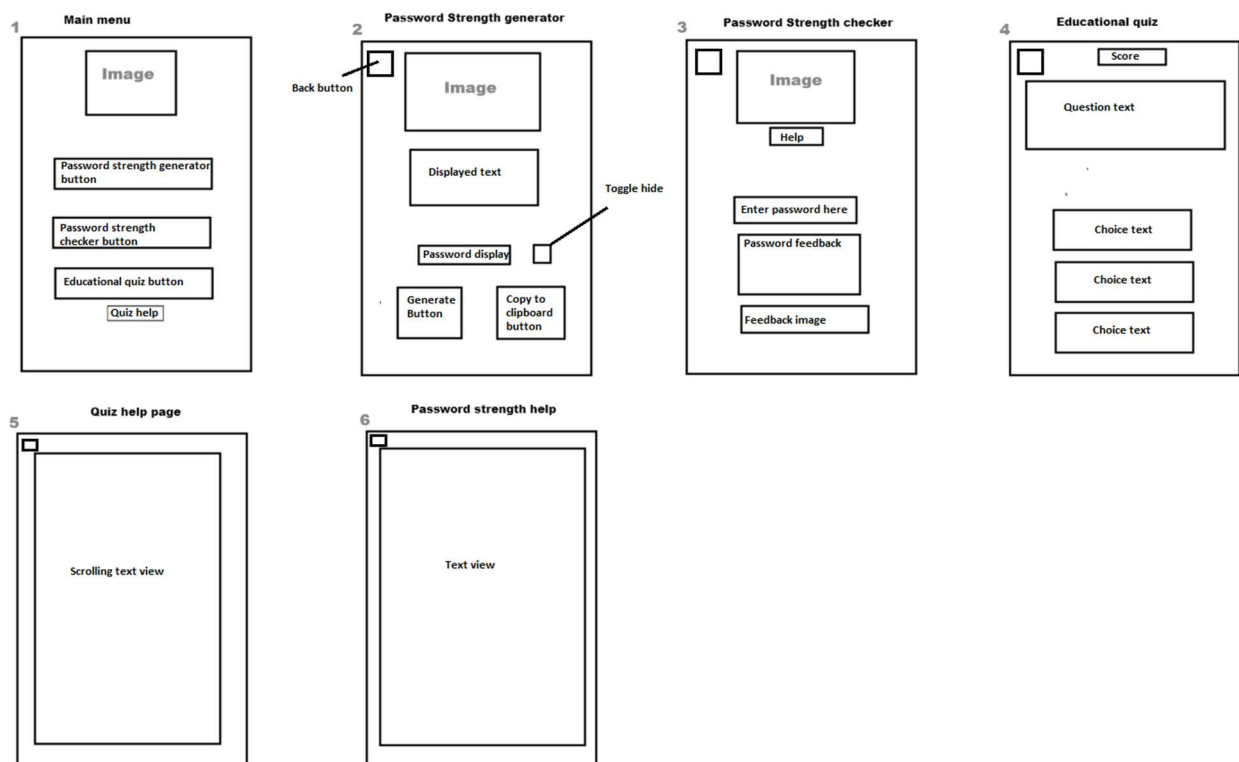
One ethical issue that may be brought up is the users typing in sensitive data i.e. passwords into the application while making use of the password strength checker. This issue is not a problem as the application has no functionality to save or store users data when typed in. The password strength checker and generator both contain a feature where a user can click to hide the password they are currently typing in for extra safety measures.

Project Development

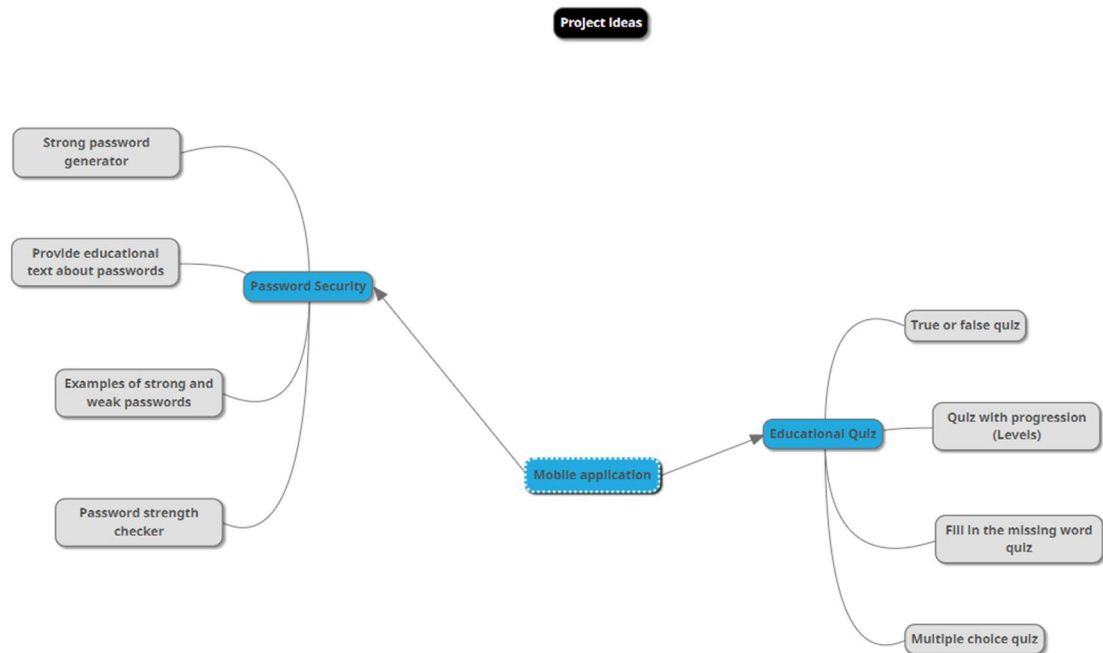
Design and Planning

During the design phase I made use of various tools to create a clearer idea and gain a better understanding of what the application I am creating would look like and how it would flow. Implementing good human computer interaction qualities is very important when designing the user interface for an application as it makes the application easier to understand and allows the user to have a more pleasant experience. Implementing poor HCI qualities into your design can leave the users having an unpleasant experience because they may have difficulty understanding what to do as the interface is not clear and user friendly.

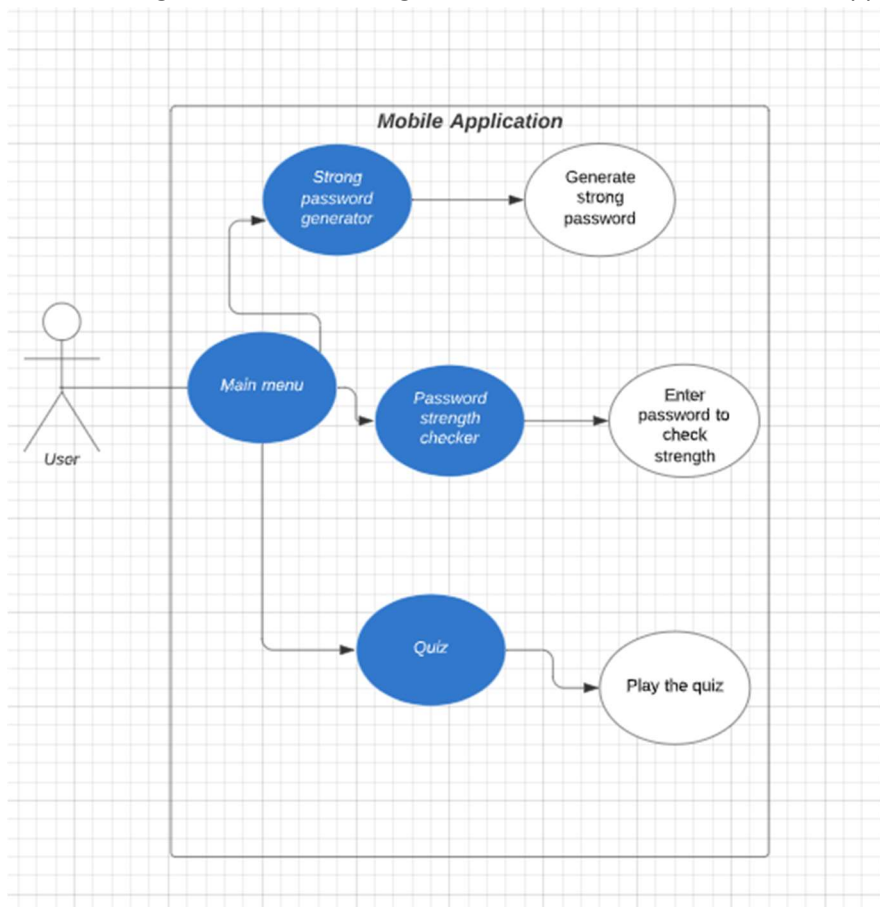
First stage of the design was creating a storyboard for the application itself and how I want to look like it in android studio. Image of storyboard below.



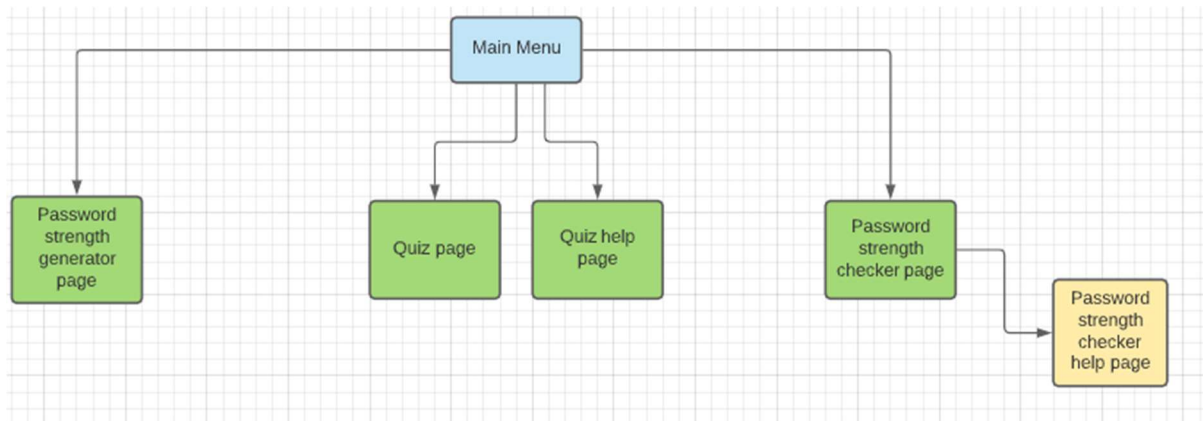
Project mind map can be seen below. I created a mind map to brainstorm potential ideas for the application.



Use case diagram below. Showing how the user will interact with the application.



UML diagram showing the overall flow the application.



Usability testing forms

Below are screenshots of the usability testing questionnaire I created. This was for getting feedback from users testing the application. Constructive feedback will allow me to make changes to more suit the users' needs. If I have had an oversight with the design or functionality of the application. Another benefit to usability testing is any bugs can get found and fixed before the application gets published.

Usability testing questionnaire

Questionnaire for usability testing feedback for mobile app "Cyber multi tool"

Overall I am satisfied with how easy the app was to use

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

The application buttons were clear and concise

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

The layout design made it easy to navigate

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

You found it easy to generate a strong password

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

You found the password strength checker easy to use

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

You found the quiz easy to use

	1	2	3	4	5	6	7	8	9	10	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

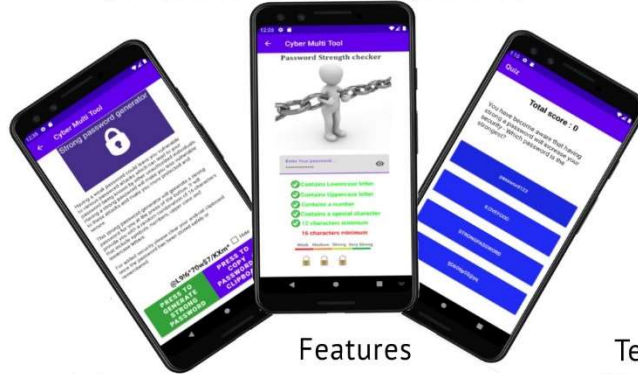
Did you come across any errors/bugs while using this application?

Long answer text

Project poster

Below is an image of the poster I designed about the project. This poster's purpose was to showcase my project and give others insight into what it is about.

CyberSecurity multifunctional app Improve personal security & security awareness



About

Cybercrime is increasing and human error can lead to security risks unintentionally through not being aware of cyber security threats or having poor security practices. This application provides users the ability to improve their personal security and increase their cyber security awareness.

Features

- Easy to use Password strength checker
- Easy to use Strong password generator
- Informative cybersecurity quizzes

Technology used

This mobile application was developed in android studio using the programming language java.

Lee Cadman

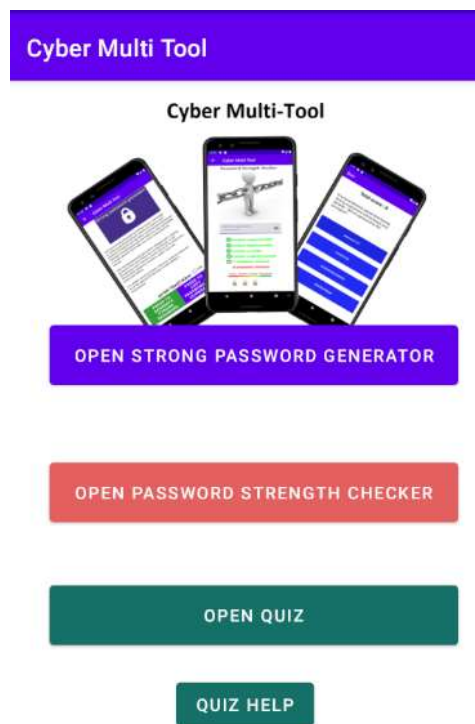
Lee.cadman@students.plymouth.ac.uk
BSc (Hons) Computer and information security
2020/2021



Complete application design and feature discussion

With the help of the design and planning phase I was able to create my original application design accurately and create a user friendly interface that was easily navigable. The application was designed to work on a wide range of android mobile devices with the compatible versions being Jellybean 4.1 – android 10. I will now show images of the completed application and discuss the features and their logic.

Main menu

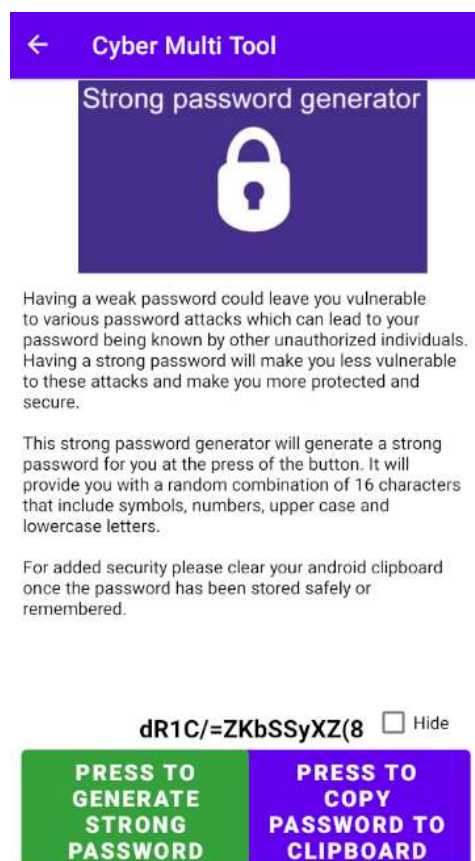


The main menu consists of 4 buttons.

- “Open strong password generator” this button allows the user to access the strong password generator part of the application once pressed.
- “Open password strength checker” this button allows the user to access the password strength checker part of the application once pressed.
- “Open quiz” this button allows the user to access the password strength checker part of the application once pressed.
- “Quiz help” this button allows the user to access the quiz help part of the application once pressed.

The main menu layout was designed to be easy on the eyes and easy to navigate for the user being clear and concise.

Strong password generator



The strong password generator will allow users to generate a 16 character long strong password at the press of a button that consists of

- Lower case letters a-z
- Upper case letters A-Z
- Numbers 0-9
- Special characters [!@#*\$%&.^&+=]

The user has the option to make use of the hide check box which will hide their generated password.

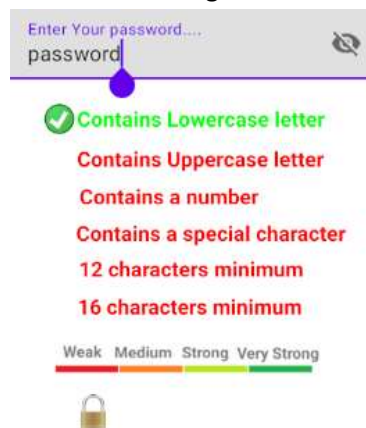


The user also has the ability to copy the password to the android clipboard at the press of a button.

Password strength checker



The password strength checker will allow users to enter a password and check the strength of the password they had entered. Responsive feedback will be prompted as the password is being entered this is in the form of text turning red to green, green ticks and padlocks appearing to indicate strength levels.



The user has the option to make use of the hide text icon which will hide their text entered.



← Cyber Multi Tool

A strong to very strong password will contain at least 12 to 16 characters and will use a mixture of uppercase (A B C) and lowercase characters (a b c), numbers (321) and special symbols (@\$%!).

Having a password that does not contain memorable dates or personal information will also make the password more secure.

Avoid using the same password on multiple websites/accounts as this puts your other accounts/websites at risk if your password gets compromised.

If the user needs help they can click the “Help button” and this will open up a new page and display information about passwords and security that can guide the user.

Educational quiz

← Cyber Multi Tool

Score: 4

Which of these scenarios is a common example of a 'phishing' attack?

Both scenarios are common examples of phishing attacks

You receive an email claiming to be from your bank asking you to enter your bank account details to receive unclaimed money

You receive a text message asking you to click a link to pay for your postal delivery

The educational quiz allows users to take part in a quiz that has questions based on cyber security risks and good cyber security practices. The quiz is multiple choice and displays 3 buttons/choices for the user to choose from to pick the correct answer. The questions, choices and score will continue to update until the user chooses the incorrect answer. When an incorrect answer is chosen a game over box will pop up and tell the user their score and give them the choice to go to the main menu or start a new game.

Score: 7

You receive a text saying your paypal account has remaining debts to pay off please click this link to log in, what should you do?

Game Over, that answer was incorrect!
Well done your score is 7 points.

[MAIN MENU](#) [NEW GAME](#)

← Cyber Multi Tool

This page will contain information that will help you answer questions on the multiple choice quiz

Passwords

- You should never share your password as this compromises the security of your accounts as you do not know what the person will do with your account. Being the only one with knowledge of the password you can assure you are the only one with access to the accounts.

- A strong password will contain at least 12 characters and will use uppercase and lowercase characters, numbers and special symbols. Having a password that does not contain memorable dates or personal information will also make the password more secure.

- It is never a good choice to reuse your password for other website because if your password has been compromised for one website/account the rest of the websites and accounts are at risk also due to having the same password.

- Bad password practice would be writing it down or saving the password into a text file, these methods could result in

If the user is having trouble choosing the correct answers in the quiz due to lack of knowledge. There is a quiz help button available on the main menu.

OPEN QUIZ

QUIZ HELP

This will take the user to a quiz help page that contains information that will help them answer the questions on the multiple choice quiz. Information is provided as the quiz's main aim is to educate the user and by providing the information all in one place the hope is that the user will learn as they read and try the quiz again.

Educational quiz questions and research

Repetition is great for learning and retaining knowledge (Repetition and Learning | Encyclopedia.com, n.d.). My hope for this multiple choice quiz is to increase the user's cyber security awareness and personal security practices through the form a education quiz with the element of repetition.

For the quiz topics I decided to cover a range of the common cyber security risks, good cyber security practices and methods of attack used by cybercriminals.

Quiz questions and research

Question : When is it okay to reuse a password?

Choice 1 : When you are using social media websites.

Choice 2 : Never.

Choice 3 : When it is too hard to remember a long password.

Correct Choice = "Never"

Research – It is never a good choice to reuse your password for other website because if your password has been compromised for one website/account the rest of the websites and accounts are at risk also due to having the same password. (Ubaid, 2020)

Question : Who is responsible for upholding good cyber security practices?

Choice 1 : Everyone

Choice 2 : Cyber-security professionals

Choice 3 : No one

Correct Choice = "Everyone"

Research – It is not just cyber-security professional's responsibility for upholding good cyber security practices, everyone in the organisation has a part to play. This gives the best chance for strong security and less chance of cyber security incidents to occur if everyone is following good cyber security practices. (Barge, 2021)

Question : What is the best way to improve a weak password such as Elephant321

Choice 1 : Add an extra number

Choice 2 : Add an extra character + Number

Choice 3 : Add multiple characters + symbols + numbers

Correct Choice = "Add multiple characters + symbols + numbers"

Question : Having a strong password will increase your security. Which password is the strongest?

Choice 1 : Password123

Choice 2 : Pets name

Choice 3 : !JO6O6p55@yq

Correct Choice = "!JO6O6p55@yq"

Question : For a more secure password, what should you make sure your password contains?

Choice 1 : Memorable dates and names

Choice 2 : Capital letters only

Choice 3 : A mixture of upper and lower case letters, symbols and numbers

Correct Choice = "A mixture of upper and lower case letters, symbols and numbers"

Research – A strong password will contain at least 12 characters and will use uppercase and lowercase characters, numbers and special symbols. Having a password that does not contain memorable dates or personal information will also make the password more secure. (How Do I Create a Strong and Unique, n.d.)

Question : You have a suspicion that your personal email account has been compromised, what should you do?

Choice 1 : Immediately reset your password, change security question and monitor for fraudulent activity

Choice 2 : Respond to the suspicious email you have received

Choice 3 : Delete the email and hope nothing comes from it

Correct Choice = "Immediately reset your password, change security question and monitor for fraudulent activity"

Research – If your email has been hacked or you have a suspicion there are steps that should be taken to ensure you have full control back over your account. These steps are reset your password, change security question and monitor for fraudulent activity. (Johnson, n.d.)

Question : What is malware?

Choice 1 : Malicious software typically used by cybercriminals to cause damage to computer systems or steal sensitive data for financial gain

Choice 2 : Anti-virus software

Choice 3 : A piece of hardware inside a computer

Correct Choice = “Malicious software typically used by cybercriminals to cause damage to computer systems or steal sensitive data for financial gain”

Question : The best defence against malware is?

Choice 1 : Regularly update all devices, software and back up data

Choice 2 : Buy cyber-security insurance

Choice 3 : Run a virus scan once a month

Correct Choice = “Regularly update all devices, software and back up data”

Research – Malware which is shorthand for malicious software contains malicious code that is usually developed by cybercriminals. Malware is typically used by cybercriminals to cause damage to computer systems or steal sensitive data for financial gain. Backing up your data and making sure all your devices and software are updated regularly will decrease the likelihood of being a victim of malware attacks. (What is malware and why do cybercriminals use malware? | McAfee, n.d.)

Question : Best method of storing a password is?

Choice 1 : Write it down

Choice 2 : Using password manager software

Choice 3 : Save in a text file

Correct Choice = “Using password manager software”

Research – Bad password practice would be writing it down or saving the password into a text file, these methods could result in your password being easily discovered and your accounts being

compromised. Good password practice would be using password manager software to store your password in securely. (How Do I Create a Strong and Unique, n.d.)

Question : Which of these below is the best for maintaining your online digital privacy?

Choice 1 : Not sharing personal information on social media

Choice 2 : Unsubscribing from spam emails

Choice 3 : Only sharing personal information with those who ask through private messages on social media

Correct Choice = "Not sharing personal information on social media"

Question : Sharing your personal/sensitive information online could make you at risk of?

Choice 1 : Worms

Choice 2 : Malware

Choice 3 : Identity theft

Correct Choice = "Identity theft"

Research – Individuals sharing their personal information online could result in them becoming a target of identity theft. Identity theft is where the attacker could use the personal information to impersonate the target individual and use their information to commit crimes. Not sharing any personal/sensitive information online is the best action to prevent this and maintain online digital privacy. (Bridges, 2016)

Question : Which of these scenarios is a common example of a 'phishing' attack?

Choice 1 : Both scenarios are common examples of phishing attacks

Choice 2 : You receive an email claiming to be from your bank asking you to enter your bank account details to receive unclaimed money

Choice 3 : You receive a text message asking you to click a link to pay for your postal delivery

Correct Choice = "Both scenarios are common examples of phishing attacks"

Question : Which type of cyber-attack is usually performed through text/social media messages and emails?

Choice 1 : Worms

Choice 2 : Ransomware

Choice 3 : Phishing

Correct Choice = "Phishing"

Question : You receive an email that looks like it's from amazon and says you have been sent an £50 amazon giftcard and it has been added to your account, click the link to spend it. What should you do?

Choice 1 : Manually go to the official amazon website on another tab to check

Choice 2 : Click the link displayed in the email to spend your gift card

Choice 3 : Forward the email to friends to show them

Correct Choice = "Manually go to the official amazon website on another tab to check"

Question : You receive a text saying your paypal account has remaining debts to pay off please click this link to log in, what should you do?

Choice 1 : Open up an internet browser and manually go to the paypal website to check

Choice 2 : Click the link displayed in the text to log in

Choice 3 : Reply to the text message

Correct Choice = "Open up an internet browser and manually go to the paypal website to check"

Question : You have just got a warning email from your bank that suspicious activity has been detected and you need to log in immediately using the URL link provided. Whats the best action to take?

Choice 1 : Contact your bank using the contact number on the back of your debit/credit card

Choice 2 : Click the link to log in and find out whats going on

Choice 3 : Reply to the email

Correct Choice = "Contact your bank using the contact number on the back of your debit/credit card"

Research – Phishing is a type of attack used by cybercriminals. It involves targeting individuals with the aim of getting them to click on a link to try and get them to hand over sensitive information or installing malware. The link can appear to be legitimate and appear to be from widely used websites such as amazon ,paypal, banking services and it will prompt the target to log in with their personal details for the attacker to then steal. Common features of phishing emails and texts are, too good to be true offers that catch the targets attention, sense of urgency, hyperlinks, attachments, unusual sender. Being cautious about the communications you receive and not clicking any direct links in messages sent by someone unfamiliar are good practices to have in defence of phishing but manually navigating to your familiar website(amazon, PayPal, banking services) to log in yourself through the address bar is the best. (Phishing | What Is Phishing?, n.d.)

Question : When visiting a website there are many checks to do to show the website is secure, one of these checks can be seen in the address bar. In the address bar which icon can be seen to show that the website could be secure?

Choice 1 : A Padlock

Choice 2 : A Door

Choice 3 : A shield

Correct Choice = A padlock

Research – A padlock in the website address bar represents the webpage has secure socket layer(SSL) installed this will usually indicate the website is secure. Looking for a green padlock that displays SSL information is just one of the many checks you should do as it is not a complete confirmation of security as some cybercriminals can use security certificates on their fraudulent unsecure websites because hosting providers do not have resources to check every new site. (Arntz, 2018)

Question : You are on your lunch break at work and you notice a work USB stick on the floor outside, what should you do?

Choice 1 : Leave it where it is

Choice 2 : Hand it in to your works IT team for them to deal with

Choice 3 : Take it home and plug it in to try and find who it belongs to

Correct Choice = “Hand it in to your works IT team for them to deal with”

Research – When finding a USB stick at work the best solution is to hand it into the IT team to deal with as they will know the correct way to deal with it. It is not safe to plug an unknown USB stick into a computer system as it could contain malicious software added by cybercriminals with the intention of causing harm to the system. (Talamantes, n.d.)

Question : You receive an email from an unrecognisable address and it says you are entitled to claim a large amount of money, please click the link to claim. What should you do?

Choice 1 : Report and block the email

Choice 2 : Click to claim your money

Choice 3 : Forward the email to friends and family

Correct Choice = “Report and block the email”

Question : How do cyber criminals usually trick others into infecting their own computer with ransomware?

Choice 1 : Clicking links in spam emails

Choice 2 : Visiting malicious websites

Choice 3 : Cyber criminals use both these methods

Correct Choice = "Cyber criminals use both these methods"

Question : You discover your computer you have been working on from home has been infected with ransomware and you cannot access your files and the hacker is demanding you to send 0.2BTC to remove it. What should you do?

Choice 1 : Pay the ransom to get your files back

Choice 2 : Disconnect your computer from the network and contact the work IT department

Choice 3 : Turn the computer off and hope it has gone the next day

Correct Choice = "Disconnect your computer from the network and contact the work IT department"

Research – Ransomware is a type of malware and is used to encrypt a victim's files or computer. The attacker can then make payment demands from the victim to decrypt the victim's files, usually asking for it to be paid in bitcoin. Ransomware is commonly delivered via emails via spam phishing emails or malicious websites tricking users into downloading a file. (Fruhlinger, 2020)

Question : Who should you share your password with?

Choice 1 : Close friends

Choice 2 : Work colleagues

Choice 3 : No one

Correct Choice = "No one"

Research – You should never share your password as this compromises the security of your accounts as you do not know what the person will do with your account. Being the only one with knowledge of the password you can assure you are the only one with access to the accounts. (Earp, 2017)

Question : How often should you run a full virus scan?

Choice 1 : At least once a week

Choice 2 : Once a month

Choice 3 : Once a year

Correct Choice = "At least once a week"

Research – Running a full virus scan at least once a week will help towards keeping your device healthy and malware free. (Allen, 2020)

Question : Who are hackers?

Choice 1 : Hackers are malicious computer criminals

Choice 2 : Computer Experts

Choice 3 : Hackers could be either ethical computer experts or malicious computer criminals

Correct Choice = "Hackers could be either ethical computer experts or malicious computer criminals"

Research – Hacking is a popular method of attack for cyber criminals and the attacker could steal information or money and cause damage to a business or person. Although hacking is usually spoken about for malicious purposes, it could also be used to improve the security of computer systems and networks where ethical hackers who are computer experts find the vulnerabilities and fix them therefore preventing possible future hacks from happening. (What Is Hacking? | What You Need To Know About Hackers, n.d.)

Question : A message has popped up while you are browsing the internet and it says you are a lucky winner and need to click to claim your prize, what should you do?

Choice 1 : Celebrate winning a prize

Choice 2 : Click the link to claim the prize

Choice 3 : Close down your internet browser/tab

Correct Choice = "Close down your internet browser/tab"

Research – Pop up messages saying you have won a prize are a scam that try to get the user to click them. Closing down the internet browser or tab completely is good solution to dealing the situation. (Pilici, 2020)

Question : You have just got home and realised you have left your phone on the bus, you have tried ringing but no get no answer what should you do?

Choice 1 : Call the phones network to let them know

Choice 2 : Remotely disable/wipe your phone

Choice 3 : Leave a voicemail with your personal details

Correct Choice = “Remotely disable/wipe your phone”

Research – There are a lot of sensitive and personal data stored on mobile phones. Most smartphone have the option of remotely disabling or wiping you phone which would be the best course of action to stop your information being compromised. (How to Remotely Disable Your Lost or Stolen Phone, 2012)

Question : What is Two-factor authentication(2FA)?

Choice 1 : When enabled 2FA adds an extra layer of security to your account by providing an additional login credential

Choice 2 : A waste of time, I want to log in fast

Choice 3 : Virus scanning software

Correct Choice = “When enabled 2FA adds an extra layer of security to your account by providing an additional login credential”

Research – 2FA adds an extra layer of security to your account by providing an additional login credential. This will make your account more secure as you will need more then just the typical user name and password to log in as it will prompt you to provide another piece of information before you can gain access. (What Is Two-Factor Authentication (2FA)? - Authy, n.d.)

Experiment, user results and findings

Users

I selected 10 people to use the application (Close friends and family who are not vulnerable and over 18 years old). These 10 individuals had no IT background or IT related qualifications, this was purposely done as my application is built mainly to educate individuals that may not have the good cyber security practices or good password practices already.

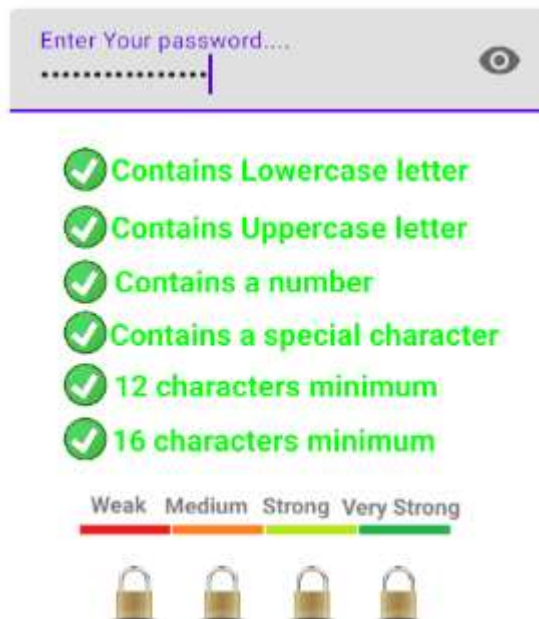
Aims and hypothesis

hypothesis – The majority of tested individuals will have a weak to medium strength password due to their non-IT backgrounds and lack of strong password practices.

Tools used – Android mobile with the Cyber Multi Tool application I developed.

Password strength checker –The test was to get each user to use the password strength checker on the mobile application I developed. It was made clear they are to create a completely new password they would consider “a strong and secure password” and type it in. The password strength checker allows the password typed in to be hidden so it was not visible to anyone including myself, only the user will know what they typed in. The application also does not store or save user data and the user cleared their text after the password strength indicator was examined and recorded down.

Example screenshot below.



The aims of this were to find out the results of my hypothesis and also to possibly show the individuals selected that their idea of what a strong and secure password is may not be correct and prompt them to change their personal passwords when they are back home to something more secure going off the knowledge they had gained from using the application.

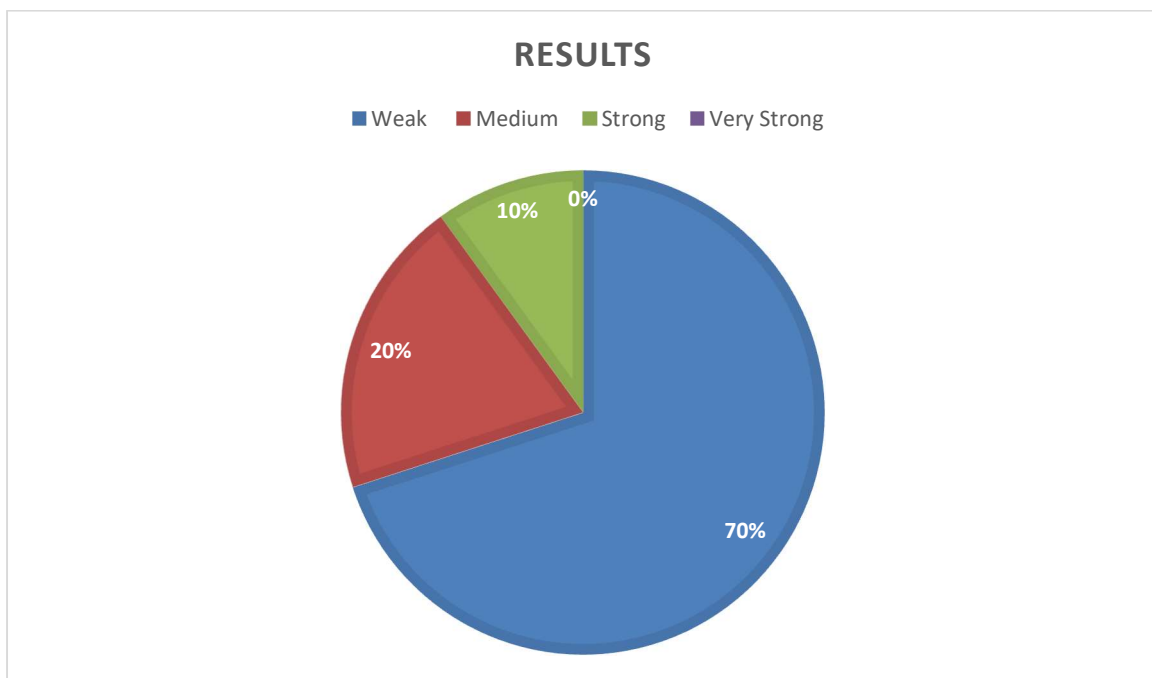
(Please note it was made clear at the end to each individual that this test itself if done by an unethical person could result in that person gaining insight into the users password practices and this could potentially comprise their real passwords)

Table of results :

User	Result
1	Weak
2	Weak
3	Weak
4	Medium
5	Weak
6	Weak
7	Medium

8	Strong
9	Weak
10	Weak

Strength	Outcome
Weak	7 Users
Medium	2 Users
Strong	1 User
Very Strong	0 Users



Discussion and Conclusion – With 70% of the users showing as having weak passwords the result is not surprising as many sources online say it is common for individuals with no IT related background to have weak passwords due to not being made aware of what good password practices are. While the sample size is small and cannot be taken as a completely proven hypothesis, the results found do aid towards proving the hypothesis right and a larger size study would be required to more accurate.

End of project reflection

Github Link - <https://github.com/CadL94/COMP3000Project>

Youtube video link - <https://youtu.be/y336JabwX0U>

Aims and Objectives met

The aims and MVP objectives set out at the start of the project were all met, these were :

I aim to produce:

- a) An android mobile application that contains the following features :
 - Strong password generator – Generates a strong password for the user with the press of a button.
 - Educational Quiz – Multiple choice quiz.
 - Password strength checker – Allows the users to check the strength of an entered password.
- b) Results from a small experiment involving an aspect of my application.
- c) Final project report that includes all aspects of my project from beginning to end.

The minimum viable product is an android mobile application that has :

- a) A Strong password generator.
- b) A password strength checker.
- c) A educational quiz.

The potential future objectives were not met due to unforeseen circumstances and the project taking longer to complete then expect. These were :

- a) Different types of educational quizzes.
- b) Extra features that improve upon personal security such as a file encryption/decryption feature.

What went well

The project application development process was done with little to no problems. The MVP objectives and aims that were set out to be done at the start were all successfully implemented and achieved. Developing the application in android studio went smoothly and this is credit to its user friendly IDE and developer features.

What didn't go well

The original method of sprint planning did not go well, and I had to change the approach due to unforeseen circumstances that occurred to better suit the situation I was in. Instead of conducting sprints every 2 weeks I had changed it to 4 weeks, while this was done to benefit my mental health at the time it did result in the project taking longer to complete than expected. The effects of a global pandemic and a lengthy lockdown on an individual's mental health were not considered in my risk analysis and that was a mistake in my part.

What would I do differently

It's hard to say what I would do differently because the circumstances would probably be different as the global pandemic caused by covid-19 will eventually fade and life will get back to normal with the university open again all year round. If the project were to occur given the same circumstances I would improve the initial planning to ensure the project was completed at a more reasonable date and not later than expected.

Conclusion

In conclusion, I feel proud to have developed the application that I had set out to create. The functionalities I wanted were all met and working smoothly. I also improved my java programming abilities as I had to learn along the way when building an application on my own for the first time from the beginning.

With cybercrime increasing yearly more should be done to educate users of computer systems and other devices. If more awareness and training was conducted by small or big companies and businesses or through social media platforms to target individuals who have non IT backgrounds there may be seen an overall yearly decrease in cybercrime instead of yearly increase.

References

Morgan, S., 2020. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. [online] Cybercrime Magazine. Available at: <<https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>> [Accessed 12 March 2021].

Accenture. n.d. The cost of cyber crime. [online] Available at: <https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf> [Accessed 12 March 2021].

Ahola, M., n.d. The Role of Human Error in Successful Cyber Security Breaches. [online] Blog.usecure.io. Available at: <<https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>> [Accessed 12 March 2021].

Nationalcrimeagency.gov.uk. n.d. Cyber crime. [online] Available at: <<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>> [Accessed 12 March 2021].

Hill, M., 2020. 90% of UK Data Breaches Due to Human Error in 2019. [online] Infosecurity Magazine. Available at: <<https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/>> [Accessed 12 March 2021].

GOV.UK. n.d. Data protection. [online] Available at: <<https://www.gov.uk/data-protection>> [Accessed 10 April 2021].

McAfee. n.d. What is malware and why do cybercriminals use malware? | McAfee. [online] Available at: <<https://www.mcafee.com/en-gb/antivirus/malware.html>> [Accessed 15 April 2021].

Ubaid, M., 2020. Why you should never reuse a password | Tom's Guide. [online] Tomsguide.com. Available at: <<https://www.tomsguide.com/uk/reference/why-never-reuse-password>> [Accessed 15 April 2021].

Barge, H., 2021. Who is responsible for Cyber Security? - Risk Evolves. [online] Risk Evolves. Available at: <<https://www.riskevolves.com/responsible-cyber-security/>> [Accessed 15 April 2021].

Webroot.com. n.d. How Do I Create a Strong and Unique. [online] Available at: <<https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password>> [Accessed 15 April 2021].

Johnson, A., n.d. 4 Things To Do If Your Email Account Is Hacked. [online] Us.norton.com. Available at: <<https://us.norton.com/internetsecurity-malware-what-to-do-if-your-email-is-hacked.html>> [Accessed 15 April 2021].

McAfee. n.d. What is malware and why do cybercriminals use malware? | McAfee. [online] Available at: <<https://www.mcafee.com/en-gb/antivirus/malware.html>> [Accessed 15 April 2021].

Bridges, J., 2016. Top 10 reasons to keep your personal information private | ReputationDefender. [online] ReputationDefender. Available at: <<https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private>> [Accessed 15 April 2021].

Talamantes, J., n.d. USB Drop Attacks: The Danger of "Lost And Found" Thumb Drives | RedTeam Security. [online] Redteamsecure.com. Available at: <<https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives>> [Accessed 15 April 2021].

Fruhlinger, J., 2020. Ransomware explained: How it works and how to remove it. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>> [Accessed 15 April 2021].

Earp, W., 2017. Why sharing passwords is a bad idea. [online] Swgfl.org.uk. Available at: <<https://swgfl.org.uk/magazine/why-sharing-passwords-is-a-bad-idea/>> [Accessed 15 April 2021].

Allen, J., 2020. 5 reasons you should run an antivirus scan at least once each week. [online] Windows Central. Available at: <<https://www.windowscentral.com/5-reasons-you-should-run-antivirus-scan-least-once-each-week>> [Accessed 15 April 2021].

Arntz, P., 2018. HTTPS: why the green padlock is not enough - Malwarebytes Labs. [online] Malwarebytes Labs. Available at: <<https://blog.malwarebytes.com/101/2018/05/https-why-the-green-padlock-is-not-enough/>> [Accessed 15 April 2021].

Phishing.org. n.d. Phishing | What Is Phishing?. [online] Available at: <<https://www.phishing.org/what-is-phishing>> [Accessed 15 April 2021].

Malwarebytes. n.d. What Is Hacking? | What You Need To Know About Hackers. [online] Available at: <<https://www.malwarebytes.com/hacker/>> [Accessed 16 May 2021].

Pilici, S., 2020. Remove "Congratulations You Won!" pop-up ads (Virus Removal Guide). [online] MalwareTips Blogs. Available at: <<https://malwaretips.com/blogs/remove-congratulations-you-won/>> [Accessed 16 April 2021].

PCMAG. 2012. How to Remotely Disable Your Lost or Stolen Phone. [online] Available at: <<https://www.pcmag.com/archive/how-to-remotely-disable-your-lost-or-stolen-phone-243990>> [Accessed 16 April 2021].

Authy. n.d. What Is Two-Factor Authentication (2FA)? - Authy. [online] Available at: <<https://authy.com/what-is-2fa/>> [Accessed 16 April 2021].