Universal Password Manager

First Author
Tiange Wang
University of Melbourne.
Parkville
Victoria, 3010 AU
tiangew2@student.unimelb.edu.au

Second Author
Xingping Ding
University of Melbourne.
Parkville
Victoria, 3010 AU
xingpingd@student.unimelb.edu.au

Third Author
Yijie Mei
University of Melbourne.
Parkville
Victoria, 3010 AU
yijiem@student.unimelb.edu.au

Abstract

This research paper is on the design of the advanced and multifunctional Universal Password Manager based on the Android platform, whose ultimate goal is to reinforce the password strength, promote user experiences and decrease the risk of the hacking private information. In today's network environment, there are various shopping, application and forum websites which require users to register different accounts to become their memberships to enjoy the exclusive discounts and high-quality service. However, from the questionnaire, we deduced that since people's memory is limited, most people selected the uniform password when signing up. It is no doubt that the behaviour and psychology are utilised by some hackers. Once they obtain the password of a person in a forum website, then his personal information and bank accounts are exposed. In addition, from the questionnaire, some people claimed that they ever used some over-simple passwords, such as '123456', 'abcdef' and 'qwerty'. Hence, we designed the app to store users' complicated and multiple passwords and generate a random password with high strength for users' reference. We believe our app will provide people with plenty of convenient on the aspects of password and cybersecurity.

If you have any questions, drop an email to
tiangew2@student.unimelb.edu.au.

Keywords

Password Manager, Cybersecurity, Biometrics, cloud services.

Introduction

Last year, following with a mass of LinkedIn accounts and passwords being dumped on the Internet, GitHub had become anther target of a password reuse attack [5]. An attacker tried to use lists of email addresses and passwords to log in GitHub, and these email addresses and passwords had been leaked from other online services in the past [5]. There is a new conceptual word named 'password reuse attack' on the Internet, which refers to the phenomenon that hackers try to log in to other websites and gain a series of available accounts through collecting the leaked user name and corresponding password information on the Internet. A large number of users in different sites using the same account password, so hackers can access the users' accounts in the A site to try to log in the B site [2]. As user account attacks have been increasingly occurred, there is a high demand to improve the security of user's accounts. The aim of this project is to design a password manager app to help users manage accounts and passwords, which can reduce the influences from password reuse attacks and improve the security of users' accounts.

Related works

Figure 1: The logo of the Password3.

Figure 2: The logo of the Pwd Manager.

We searched the related work and found two existing apps: one is Password 3, another is Pwd Manage.

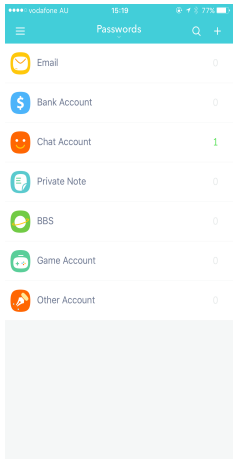


Figure 3: The screenshot of the Password3 category.

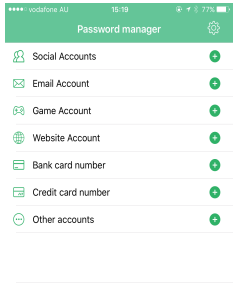


Figure 4: The screenshot of the Pwd Manager category.

As two figures shown above, all of them designed explicit lists for different accounts, such as social media accounts, bank accounts and email accounts. It is apparent for users to find the item which they would like to copy or store the password information.

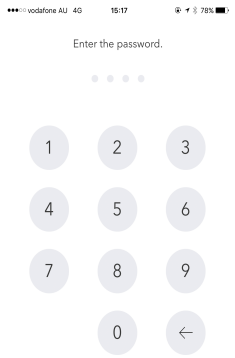


Figure 5: The screenshot of the Password3 login.

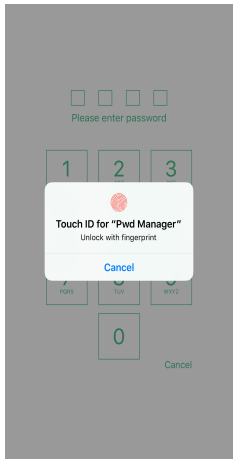


Figure 6: The screenshot of the Pwd Manager login.

Nonetheless, these two apps also have disadvantages. The access password which only contains four numbers is over-short and over-simple. Although they add the 'touch ID' to enhance the security level, some old devices, such as iPhone 5, do not have the hardware to support the "touch ID' function. In addition, as the password information is typed by users manually, they did not deal with the 'same password' issue. Meanwhile, the synchronisation function is limited in both of two apps. It implies that the passwords stored on iOS devices are not able to transfer to Android devices.

Requirements analysis

In order to acquire the actual data, we generate a questionnaire on the Surverymonkey.com. Shown in diagrams are the result of the survey, 83 percent participants encountered accounts hacked, 57.14 percent participants admit that they ever set over-simple passwords. Meanwhile, it showed the

incredible proportion of participants who set the same passwords for some websites, which reaches 88.57 percent, and among them, the reason primarily is that different and various passwords are difficult to memorise [7]. Also, 80 percent participants are willing to utilise the password manager app to manage passwords [7]. Li et al. [4] also indicated that users expect that password manager could reduce their memory fatigue.

Through the result of the questionnaire and related work, we summarised that users primarily focused on these four aspects: various password management, login security, strong password generation and backup and synchronisation. Moreover, the significant goal of the password manager is to encourage users to utilise different passwords to avoid the 'password reuse attack' issue.

Therefore, we built the app and expected it to improve the bad behaviour of users when signing in. The app contains four core functions, including access with biometrics, storing passwords, autogeneration and cloud services. We absorbed the experience of similar apps in the market and aimed at making functions interact with user experience and entertainment.

Design - Function specifications

There are four primary functions in our app.

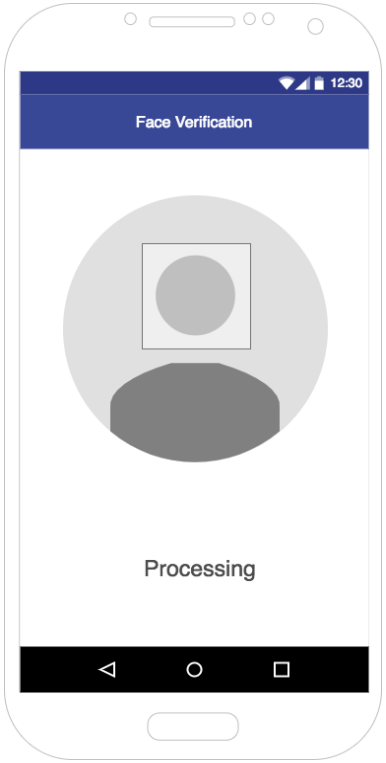


Figure 7: Face verification function interface .

The first is the **login function**. We browsed some current papers and reports and used some apps at the moment. Almost without expectation, they did not mention or add the access control function to the manager. Thus, in our opinions, as a password manager, the app should focus on not only the password storage and password security, but also the access verification and safety.

It is well-known that the biometrics authentication is a kind of access verification technology with high security due to the uniqueness of the biological feature [3]. In recent years, face verification technology has significantly improved. The DeepFace, which is a Facebook's facial recognition research project, can nearly get a accuracy as human brain [1]. The task is that the DeepFace looks at two photos and then says whether the two photos contain the same face [1]. The DeepFace can get a 97.25 accuracy, while humans perform this task with 97.53 accuracy [1]. In this project, we applied face verification instead of 'touch ID' since the cameras are widely used. Some old devices, such as iPhone 5 and Samsung Galaxy S4, are not configured touch ID function. Therefore, we added the face verification function in the access to the app. When downloading this app at the first time, the user has to sign up to become our membership as we also provided cloud services. After filling in the personal information, then click the 'Face verification' button. Waiting for the preparation of the camera, then follow the instructions to adjust the light, luminance and face position. After hearing the prompt tone, the scan operation is finished. It is similar to the operations when we play some sports games on the game consoles like PS4. The face verification technology is based on Microsoft Azure, which allows the app to upload the photo and compare with the record in the cloud server. Then the cloud server returns a value of the similarity to the app to determine whether the current user is the authentic user of these passwords.

In addition, for increasing the security coefficient, we imported the dual-factor authentication for those users who lose their phones or changes to a new phone. Hence, in the register step, we required users to leave their phone numbers to receive the verification SMS with a string of numbers from our information centre to bind the phone. When users need to change devices, they open the app and then they should not only verify their faces but also attach the security code in case of hackers who could use 3D models to cheat the biometric system.

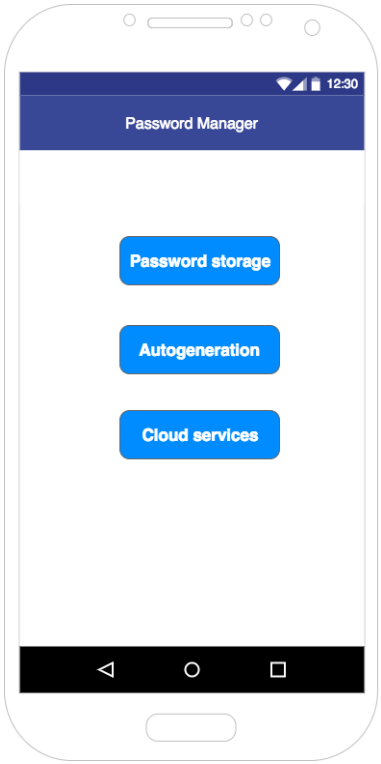


Figure 8: The main interface .

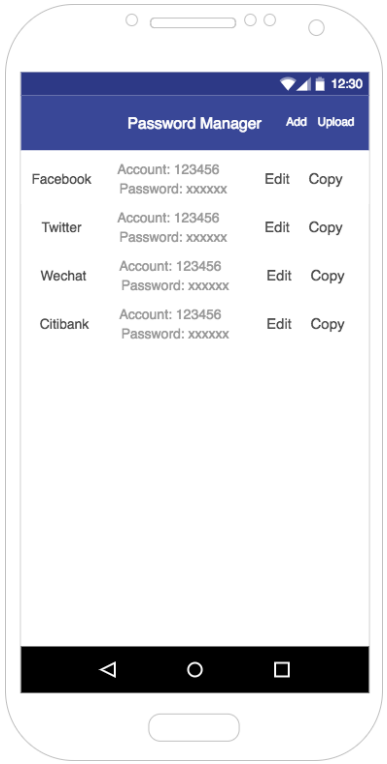


Figure 9: The password storage interface .

Next, users could see the main interface of the app, which has three buttons in the centre (Password storage, Autogeneration and Cloud services) for users to select. We click the **'Password storage'**. Shown in the figure above is the interface of the password storage function. It looks like the interface of the Excel. The first column describes the name of website, and following is the account name and password. The last column are the space for the buttons of edit and copy. Moreover, we provided users with two options, manual storage and automatic storage.

For manual storage, it is similar to operations in the Excel. If users want to add a new record, just click the 'Add' button on the top right corner and type the website name, account name and password. However, we did not suggest users do the manual operation because once the records in the database become large, the various data may make people feel dizzy.

For automatic storage, we designed a plugin which is interacted with the browser. When users log in a new website, the plugin prompts 'Do you want to save the password for this site?'. If yes, the password is stored in the database with the website name and account information instead of typing manually. Once the user tries to log in the same website, the plugin automatically fills in the login form for him. Users only require considering the password to satisfy the requirement of the site rather than memorising the password they set as the app and plugin could do all the services for them.

Meanwhile, we adopted the AES (Rijndael Algorithm) to encrypt the data in the local database. The AES has more complicated structure than other symmetric key cryptography algorithms and is utilised by the USA government due to its simple design and strong attack resistance [6]. Passwords are closely related to the private information, bank accounts and fund security. On the one hand, password manager offers the convenient and replaces user to memorise. On the other hand, we should guarantee the safety of the app itself. Hence, we integrated multi-verification and powerful encryption technology to ensure the process of password typing and storage is secure.

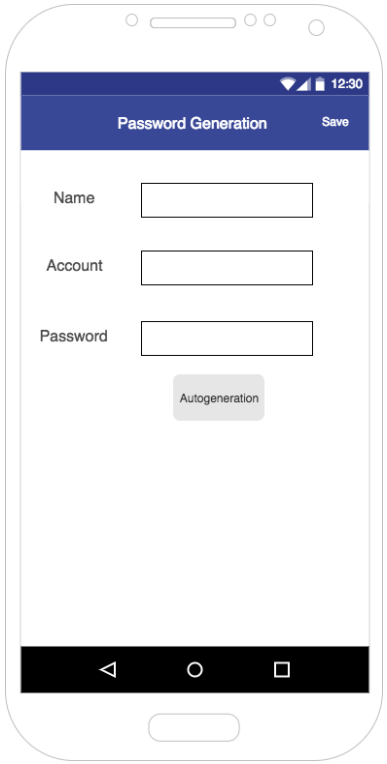


Figure 10: The password generation interface .

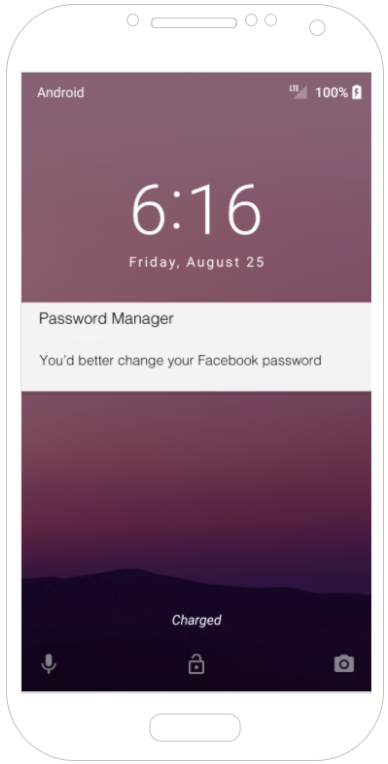


Figure 11: The push notification interface .

There is a 'back' button in the lower left corner of the screen for users to return to the main interface. Now suppose that we are in the main interface. When clicking the 'Autogeneration', we enter to the corresponding function.

'Autogeneration' primarily serves for those users who are not willing to set a secure password manually or could not catch such a password in mind. The interface of this function is correspondingly simple which contains two textboxes for

users to type the name of the websites or apps, accounts ID, a password textbox to display the password generated and a button called 'Autogeneration'. After users click it, it follows the essential rules of password setting in most forums and sites and generates a random password with series of uppercase and lowercase letters, numbers and characters. For example, 'Aaplgh1995 ' is a valid but strong password, and the app could generate similar passwords for users to select. Users are able to copy it and paste in the sites to validate it. Then it will automatically store the password record in the local database. The autogeneration aims to provide users with different strong passwords to avoid the 'password reuse attack' issue. Some users may worry about the security of the process of copying and pasting. The app will automatically encrypt the password with AES and remove the copied password information after 90's.

If users dislike this password, they are allowed to shake phones twice to gain a new password or shake them for several times until they are satisfied with it. The shake function is connected to the sensor in the phone. When users shake their phones, the sensor sends the 'shake' signal to the app and app do the generation operation. It is similar to the 'Shake' function in the WeChat app, which is a method without any practical significance that only collects user's gesture and response and increases the user experience. Teenagers may be interested in the shake function to avoid dull feelings.

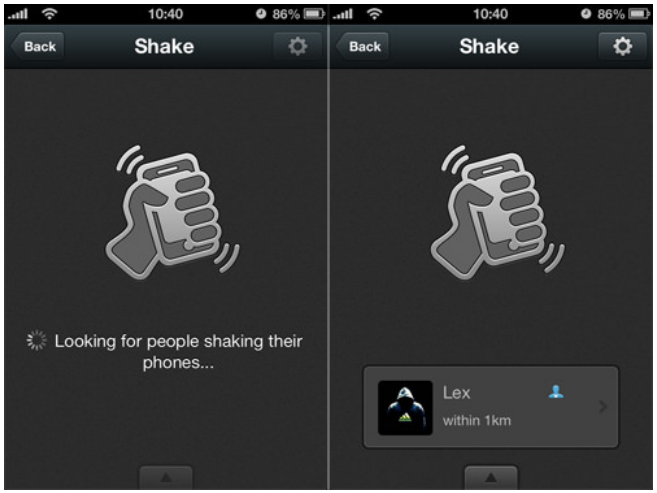


Figure 12: The screenshot of the WeChat app.

The account is unused for a long time, and the password is not altered for a long time are the significant reasons for accounts hacked [4]. Hence, we added an 'automatic reminder' function for users who do not change their passwords for three months and above.

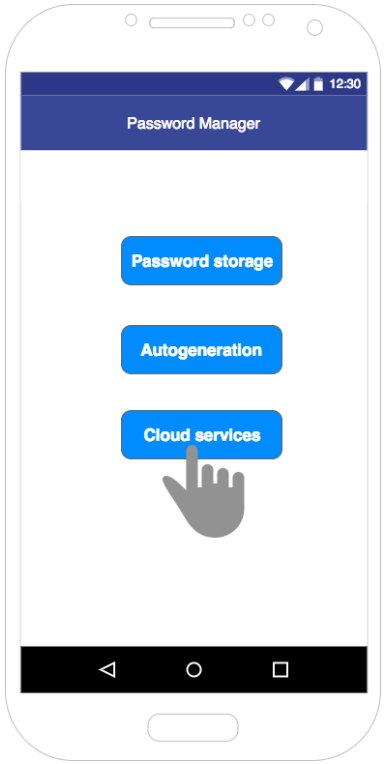


Figure 13: The cloud service interface .

Lastly, let users return to the main interface and click **'Cloud service'** button. We provide users with not only the local storage but also cloud service. In the login function, we mentioned the register and membership. The scanned face is the password to log in the cloud service. However, for promoting the security level, when users log in for the first time, we added the dual-factor authentication and mandatorily required users to receive verification SMS and type the number code in the textbox. Our server would verify the code to judge whether the request from the app is sent by authentic users.

We researched on some apps in the market, such as Keeper, Keepass and 1Password. They all offer the cloud service to users to support them to use on different platforms. The cloud service avoids the embarrassed circumstances that the phone is the only platform to utilise and log in, and when users switch the device, it implies the password is 'forgotten' as users do not memorise them in the brain. The another significant advantage when applying cloud storage is backup provided. Sometimes the local database may encounter various accidents to lead to the database breakdown or record lost. We set the 'automatic reminder' function to ask users whether they want to backup the local database.

During the uploading and downloading of the local password database, we adopted the AES algorithm to encrypt the data with 256-bit ciphertexts which effectively blocks hackers from prying. And the same encryption method is applied to our server. Hence, users are able to feel free to upload and download the passwords to synchronise the local database.

He et al.[3] also illustrated some browsers design the password storage function, however, when users change other devices, the saved passwords cannot synchronise to the new platform which makes some users have to recall and type passwords manually. Our app integrated the 'automatically type forms' function in the browsers and 'cloud storage' on the servers to prevent this situation happening.

Evaluation

In the survey, besides the questions related to information and account security, we designed a question 'Are you willing to download a password manager app to help you save and man-

age passwords?'. And 80 percent participants indicated that they would have a try on this new password manager. From the result of the survey, many people primarily concerned about the account security and expressed the consideration that they attempted to set a firm and distinct password but could not memorise them all. Thus, in the process of design, we considered and gained the experience from the survey and other apps in the market, started with login, password storage, password generation and cloud service fields to build this app. In our opinions, our app could basically deal with the trouble of memory and security risks.

After the app design finished, we invited our friends to take part in out interviews.

Mr. Martin Huang is a project manager of the Dulux company. His work is hectic, so he chooses surfing the Internet to relax. He also demonstrated his memory is too bad to memorise different passwords and had to use the same password in forums and social medias. From his selections in the survey, we knew his account in Reddit was ever stolen by hackers since he logged in a phishing website through using the Facebook account. Hence, we exclusively asked him whether he considered the app had addressed his issues. And we were glad to hear that he was satisfied with our product.

The second interviewee was Mr. Chaoyi Han. He is an MIT student in Unimelb and also a crazy fan in basketball and electronic products areas. The problem he encountered was also accounts hacked. The hackers he met was so excessive that they not only altered his passwords but also posted many spams in his name. Although he used a stronger password instead and never experienced similar accidents since then, he considered that it is necessary to download a password manager app on his phone. As an electronic product fan, he has five devices, so he loved our product especially the cloud storage and synchronisation function.

The last one is Miss Xiaoye Xiong, a student in Unimelb who studies the translation. Her circumstance is different from those two cases above. She never encountered any hacked accidents and used the secure password with alphabets, numbers and symbols all the while. She focused on the cybersecurity and gave our face verification function a high evaluation. Meanwhile, she also felt convenient as our app liberated her fingers.

Conclusion

Many users continuously use the same password due to their bad memory, which causes many accounts hacked accidents. The related news is frequently reported. For instance, the credit card information was leaked, and the net bank was consumed. We invited friends to participate in the survey through the web link or invitations on the Facebook. The result confirmed the circumstance in our lives is very common. There were only a few users having the habit of using the password manager. In addition, some password manager app does not include the cloud services which leads to increase the concerns of users. Once they switch the device, some sites they could not log in again since they forget the password. For example, if the app only provides local services, it always implies that users can only do some operations on this device.

To avoid this embarrassing situation, we designed the cloud service for users to download and update passwords anytime and anywhere from our secure server. In our opinions, our app basically figured out the accidents which are caused by the same password in our lives and satisfied with the most users' requirements. From the sample survey (interview), we received some feedbacks from actual users. From these positive feedbacks, we basically consider our app is successful

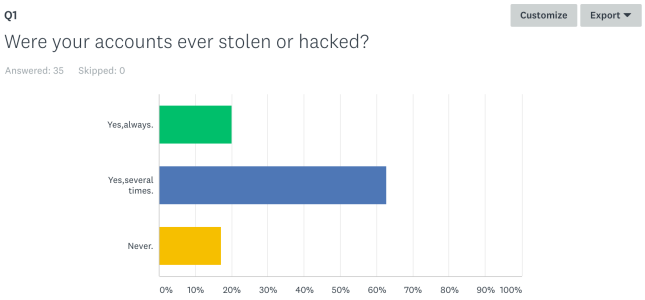
to help people memorise various and complicated passwords and reduce the possibility of the accounts hacked accidents effectively.

However, our product also has some limitations. For instance, the precision of the face verification technology. Actually, we utilised the Microsoft Azure Face Verification API which we have not assessed its efficiency and effectiveness. Moreover, if both of the twin sisters/brothers are the customer of our product, how does the app distinguish them accurately rather than approving their face verification application confusedly? We thought these potential issues and risks are worth studying and resolving in the next step.

In conclusion, we consider that our app can improve the security of users' accounts and make a safe future for users.

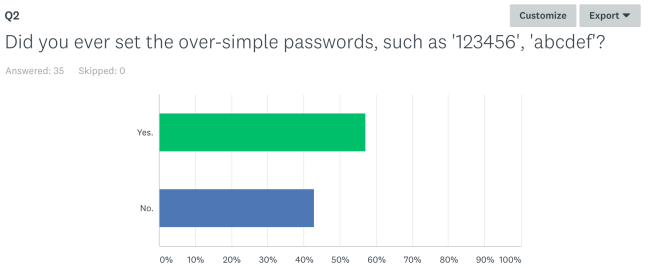
Appendix

1. The five figures below are screenshots of the **survey result**.



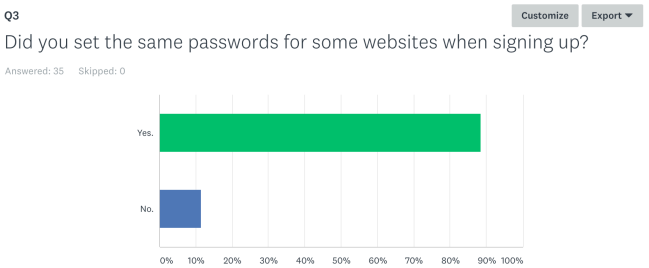
ANSWER CHOICES	RESPONSES	
Yes,always.	20.00%	7
Yes,several times.	62.86%	22
Never.	17.14%	6
TOTAL		35

Figure 14: The result of question 1 in the survey.



ANSWER CHOICES	RESPONSES	
Yes.	57.14%	20
No.	42.86%	15
TOTAL		35

Figure 15: The result of question 2 in the survey.



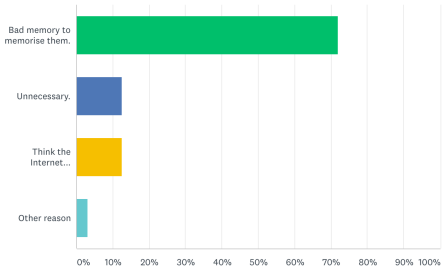
ANSWER CHOICES	RESPONSES	
Yes.	88.57%	31
No.	11.43%	4
TOTAL		35

Figure 16: The result of question 3 in the survey.

Q4 Customize Export

For those who ever set same and simple passwords, why did you do that?

Answered: 32 Skipped: 3



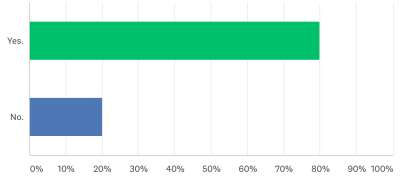
ANSWER CHOICES		RESPONSES	
Bad memory to memorise them.		71.88%	23
Unnecessary.		12.50%	4
Think the Internet environment is safe enough.		12.50%	4
Other reason	Responses	3.13%	1
TOTAL			32

Figure 17: The result of question 4 in the survey.

Q5 Customize Export

Are you willing to download a password manager app to help you save and manage passwords?

Answered: 35 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes.	80.00%	28
No.	20.00%	7
TOTAL		35

Figure 18: The result of question 5 in the survey.

2. Below that is the **interview records**.

Thanks for these three participants to accept my interview invitation.

Interviewer: Tiange Wang (Hereinafter to be referred as 'W'), Xingping Ding (Hereinafter to be referred as 'D'), Yijie Mei (Hereinafter to be referred as 'M').

Mr. Martin Huang, 26, Project Manager, Like surfing Internet. (Hereinafter to be referred as 'H').

W: What do you think on this app?

H: I love surfing the Internet and registered for many forums. However, since I am a project manager, I do not have much time on memorising various passwords and have to use the same password for many sites and social media. Now I tried your app and find it is really helpful to store passwords and save my time.

W: Do you think the app has addressed the problems in the questionnaire?

H: Yes.

W: OK. Thank you! Have a nice day!

Mr. Chaoyi Han, 22, Student in Unimelb, Basketball and Electronic products fans. (Hereinafter to be referred as 'H').

D: I remember you said you used same passwords for same sites, right?

H: Yes.

D: And you also encountered some hacked account accidents?

H: Yes. I hate hackers to alter my passwords of social medias and post some garbage messages.

D: So do you think this app help you avoid these annoying situations after one day's usage?

H: Of course. Apart from the password storage function, I should also give you a thumbs up on the cloud service. I usually switch my accounts of social media and forums between different devices. Now the cloud service satisfies my requirements.

D: Sounds good! Have a lovely night!

Miss Xiaoye Xiong, 23, Student in Unimelb, Shopaholic. (Hereinafter to be referred as 'X')
M: Oh, I just noticed you used our app to help you log in the ASOS?
X: Yes, it is really convenient. I do not need to type the password manually any more.
M: That's cool. What do you think the greatest advantage of our app?
X: Emm, you know, I am a shopaholic and I love shopping online as I can get the goods from all over the world. Thus, the information and credit card security is what I am most concerned about although I have not met any hack accidents. When I log in, the face verification technology is applied which makes me feel safe. So I think the security aspect is the good advantage of your app.
M: Cool! Thank you for the interview! Have a good day!

References

[1] S. Anthony. Facebook's facial recognition software is now as accurate as the human brain, but what now? http://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now/, 2014.

[2] P. Gasti and K. B. Rasmussen. On the security of password manager database formats., 2012.

[3] D. He and D. Wang. Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, 9(3):816–823, 2015.

[4] Z. Li, W. He, D. Akhawe, and D. Song. The emperor's new password manager: Security analysis of web-based password managers., 2014.

[5] N. Lomas. Github accounts targeted in password reuse attack. https://techcrunch.com/2016/06/16/github-accounts-targeted-in-password-reuse-attack/, 2016.

[6] W. Stallings and M. P. Tahiliani. *Cryptography and network security: principles and practice*, volume 6. Pearson London, 2014.

[7] Surveymonkey.com. Password survey. https://www.surveymonkey.com/r/DQKN7RS, 2017.