Gurugram Police Summer Internship 2020

Research/Survey Based Project

On

Password Security and Management

Submitted by:

Aniket Mathur

Indrajith Gopinathan

Shubhro Gupta

Supported by:

Society for Safe Gurgaon

SISL Infotech Pvt Ltd

Submitted to:

Mr. Rakshit Tandon

CERTIFICATE

This is to certify that **Indrajith Gopinathan** has successfully completed his group Research Project on "**Password Security and Management"**, towards the partial fulfillment of the requirements for the certification in the Cyber Security training conducted by Gurgram Police Summer Internship 2020 and is the record work carried out by him under my supervision and my guidance.

In my opinion, the submitted work has reached a level required for being accepted for the certification. The results embodied in this group project, to the best of my knowledge hasn't been submitted to any other institution or university for the award of any degree or diploma or certification.

Rakshit Tandon
Mentor/Coordinator/Advisor- Gurugram Police Cyber Security Summer Internship 2020
Director/Co Founder- HackerShala/CodesNag
Cyber Security Consultant- Internet and Mobile Association of India (IAMAI)

CERTIFICATE

This is to certify that **Shubhro Gupta** has successfully completed his group Research Project on "**Password Security and Management"**, towards the partial fulfillment of the requirements for the certification in the Cyber Security training conducted by Gurgram Police Summer Internship 2020 and is the record work carried out by him under my supervision and my guidance.

In my opinion, the submitted work has reached a level required for being accepted for the certification. The results embodied in this group project, to the best of my knowledge hasn't been submitted to any other institution or university for the award of any degree or diploma or certification.

Rakshit Tandon
Mentor/Coordinator/Advisor- Gurugram Police Cyber Security Summer Internship 2020
Director/Co Founder- HackerShala/CodesNag
Cyber Security Consultant- Internet and Mobile Association of India (IAMAI)

CERTIFICATE

This is to certify that **Aniket Mathur** has successfully completed his group Research Project on "**Password Security and Management"**, towards the partial fulfillment of the requirements for the certification in the Cyber Security training conducted by Gurgram Police Summer Internship 2020 and is the record work carried out by him under my supervision and my guidance.

In my opinion, the submitted work has reached a level required for being accepted for the certification. The results embodied in this group project, to the best of my knowledge hasn't been submitted to any other institution or university for the award of any degree or diploma or certification.

Rakshit Tandon
Mentor/Coordinator/Advisor- Gurugram Police Cyber Security Summer Internship 2020
Director/Co Founder- HackerShala/CodesNag
Cyber Security Consultant- Internet and Mobile Association of India (IAMAI)

Undertaking for Originality for the work

I, Aniket Mathur, give undertaking that the group project titled “**Password Security and Managemen**t” submitted by my group, towards the partial fulfillment of the requirements for the certificate of Gurugram Police Summer Internship 2020, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Student Name: **Aniket Mathur**
Date: **14th July 2019**

I, Indrajith Gopinathan, give undertaking that the group project titled “**Password Security and Managemen**t” submitted by my group, towards the partial fulfillment of the requirements for the certificate of Gurugram Police Summer Internship 2020, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Student Name: **Indrajith Gopinathan**
Date: **14th July 2019**

I, Shubhro Gupta, give undertaking that the group project titled “**Password Security and Managemen**t” submitted by my group, towards the partial fulfillment of the requirements for the certificate of Gurugram Police Summer Internship 2020, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Student Name: **Shubhro Gupta**
Date: **14th July 2019**

Acknowledgment

We express our sincere gratitude to Gurugram Police for providing us with an opportunity to be part of this Gurugram Police Summer Internship 2020 to complete this Research Project on ‘‘**Password Security and Management**’’.

We sincerely thank:
Sh. K.K. Rao (Commissioner of Police, Gurugram)
Ms. Nikita Gehlawat (DCP)
Ms. Pankhuri Kumar (ACP SO1)
Mr. Karan Goyal (ACP Cyber Crime)
Mr. Rakshit Tandon (Cyber Safety Advisor Cyber Crime, Director Council of Information Security, Consultant-Internet & Mobile Association of India)
Ms. Akshita Jain (Systems Engineer)

for their guidance and encouragement in carrying out this project work. We also express our gratitude. We also thank all the experts invited to GPCSSI 2020.

Lastly, we thank the almighty, our parents, our siblings, our friends, and the whole Gurugram Police Team for their constant support without which this project would not be possible.

Index

Introduction

> The definition and importance of Cyber Security

Cyber Security refers to the "*body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access*". Cybersecurity may also be referred to as information technology security.

Cyber Security is important because the government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing business, and cybersecurity describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding

information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.

> Challenges of Cyber Security

There are however numerous challenges faced by Cyber Security networks around the globe.

For effective cybersecurity, an organization needs to coordinate its efforts throughout its entire information system.

Elements of cyber encompass all of the following fields: **Network security, Application security, Endpoint security, Data Security, Identity management, Database and infrastructure security, Cloud security, Mobile Security, Disaster recovery/business continuity planning, etc.**

> What is Password Security?

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need,

on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

Using strong passwords lowers the overall risk of a security breach, but strong passwords do not replace the need for other effective security controls.

Computer users are generally advised to "*never write down a password anywhere, no matter what" and "never use the same password for more than one account.*" However, an ordinary computer user may have dozens of password-protected accounts.

Users with multiple accounts needing passwords often give up and use the same password for every account. When varied password complexity requirements prevent the use of the same (memorable) scheme for producing high-strength passwords, oversimplified passwords will often be created to satisfy irritating and conflicting password requirements.

Software is available for popular hand-held computers that can store passwords for numerous accounts in encrypted form. Passwords can be encrypted by hand on paper and remember the encryption method and key.

> The use of Password Managers?

Password managers offer greater security and convenience for the use of passwords to access online services.

Greater security is achieved principally through the capability of most password manager applications to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault. Greater convenience is provided by the use of a single master password to access the password vault rather than attempting to memorize different passwords for all accounts.

Most password manager applications offer additional capabilities that enhance both convenience and security such as storage of credit card and frequent flyer information and autofill functionality.

Password managers also help in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.

> Why is password security important?

Repeatedly using the same passwords or using ‘weak’ passwords can leave you vulnerable to hackers. If a hacker cracks your passwords, they could gain access to your social media accounts, bank accounts, emails, and other sensitive accounts that hold your confidential, personal data. If someone obtains access to this information, you could become the victim of identity theft. Therefore, creating a strong password is vital.

Password hacking is often carried out in one of the following ways:

- **Brute force attacks**: A hacker uses automated software to guess your username and password combination. The software tries every possible character combination and will try the most commonly used passwords first, so weak or common passwords can be relatively simple for a brute force attack to crack. While this method will eventually crack your password by cycling through every possibility until it matches your character combination, you can make it take a very long time by using a complex password.

- **Dictionary**: With this method of hacking, a hacker will run a defined ‘dictionary’ against your passwords. This dictionary also includes the most common password combinations, therefore it is a relatively easy and quick way of hacking into weakly protected accounts. By using a single-use, strong password for each account, you should be able to protect yourself from a dictionary hack.

- **Phishing and social engineering**: Accessing someone’s password using phishing or social engineering attack is not technically a type of hack, but it provides the ‘hacker’ with access to your passwords and confidential information. This in turn allows them to access your accounts. Phishing occurs when a hacker targets you with spoofed emails that look like they come from legitimate organizations, while social engineering is real-world phishing (i.e. over the phone).

Survey Analysis: Data/Fact breakdown

The following section provides a thorough breakdown of our conducted survey on password security.
We have done this in an interactive and structured format, as displayed below.

- **Question**
- **Critical analysis of numbers and stats received**
- **Issues posed (if any)**
- **Solutions to the issues posed above**

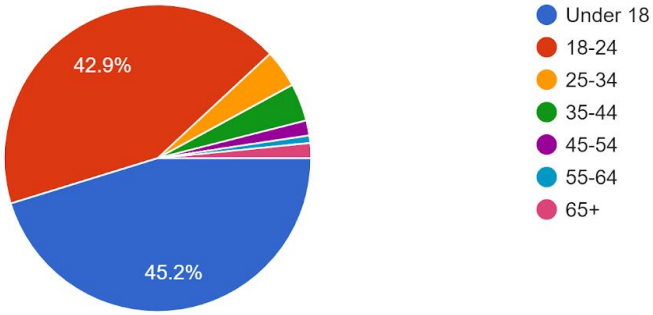
The general analysis has been broken down into 5 components, with the index as follows:

SECTION 1	General Demographics
SECTION 2	Overview
SECTION 3	Password-Specific Queries
SECTION 4	Myths vs Facts
SECTION 5	Miscellaneous and Conclusion

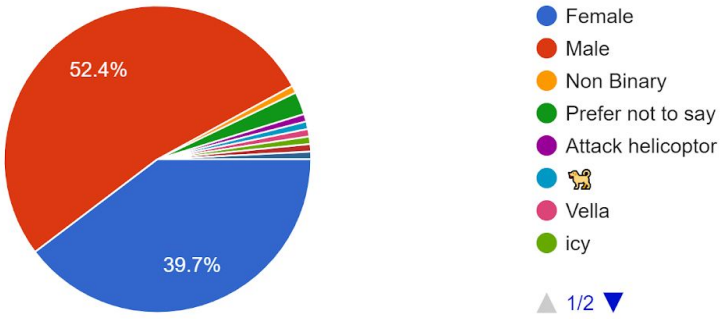
SECTION 1

> Gender/Age demographic

Age group:
126 responses



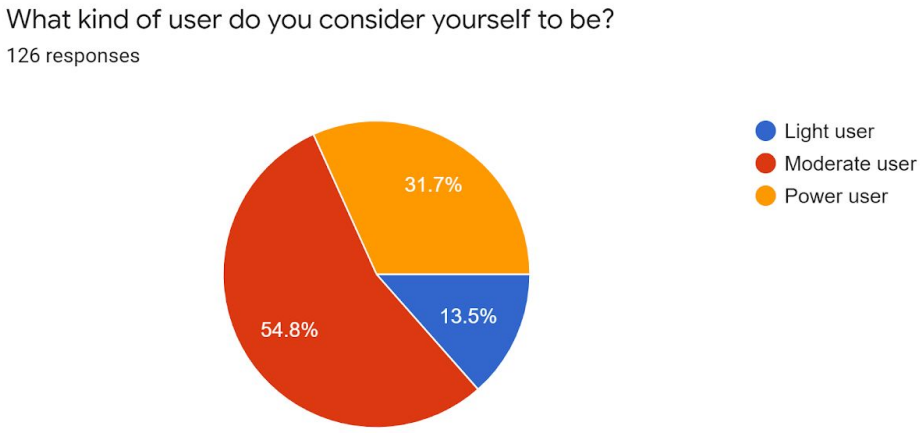
Gender:
126 responses



SECTION 2

> Overview

Q:

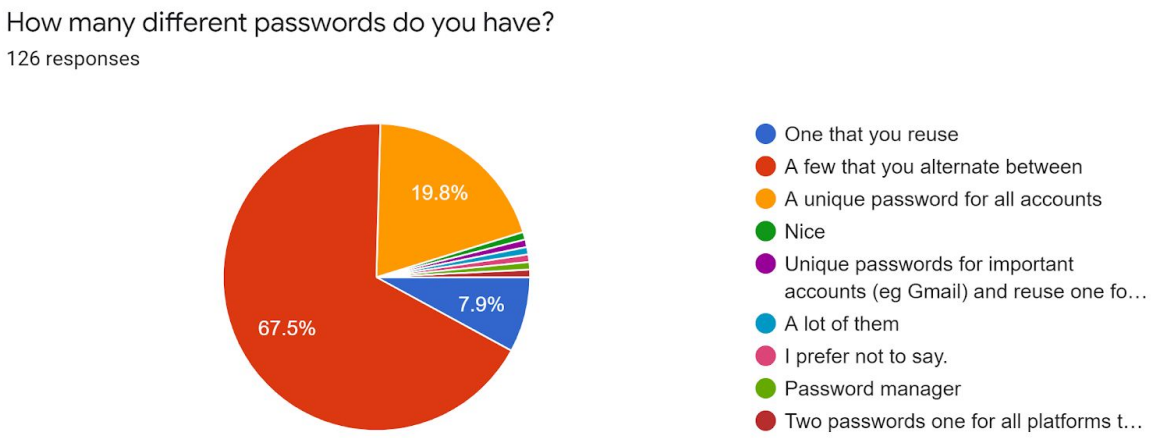


Analysis: It is quite obvious in the modern age that people around us have started to spend more time on electronic devices, and more than ever now with the onset of the pandemic.
The graphic pans out a general distribution, with maximum users in the moderate zone, followed up by about 1/3rds of them in the power or highly-intensive zone.

Q: How many password-protected accounts do you have?
Analysis: It was noticeable that almost a majority of the users have a mixture of password protected numbers lying in between the under-satisfactory and regular range.

However, such users may not have set-up their accounts on too many platforms online and elsewhere, which has led to the production of a result that is in stark contrast to users who lie in the good and over-satisfactory range pertaining to the number of protected accounts.
Issue: If the aforementioned reason isn't the actual reality, users could be prone to various threats online with accounts that are not password protected or secure.
Solution: Encouraging users to set up PPAs and spreading more awareness on the need to stay safe online with the help of such accounts is the need of the hour.

Q:

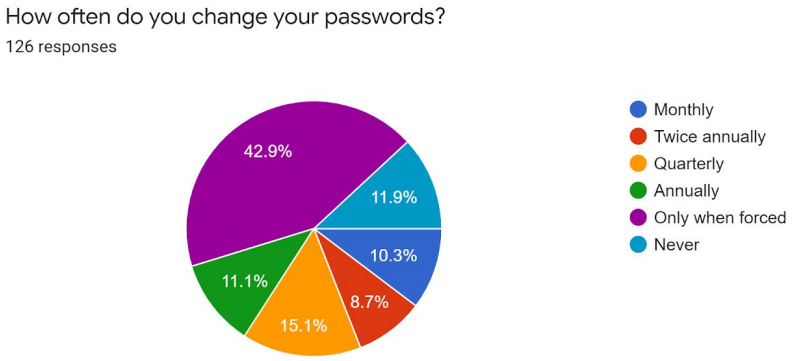


Analysis: A bit above 2/3rds of the user pool alternate between a few passwords they use on a daily basis, usually ones which are easy to remember and are convenient. In some cases, the passwords may have been well crafted.

Almost one-fifth of the users actually use different passwords for different accounts and platforms, which while providing the best security also becomes slightly tedious to manage. The third most significant data visible is the minute chunk of users that keep reusing a single password and as such face maximum security risks.
Issue: Password managers have once again proved to be highly underrated and underused, sometimes contributed to by the complexity it poses or the general laziness of the user. The users that keep reusing the same password everywhere or alternate between a few are on the frontlines of the risk factor, as their security can be easily compromised in comparison to users who use a more diverse palette of passwords/ keep a unique one for each account they make.
Solution: As mentioned, password managers play a great role in helping users set up a large number of highly secure passwords that are convenient and easy to manage. Providing users with simple-to-use and cheap managers is the ideal solution to tackle this issue.
Also, more alternatives such as keeping personal managers for different passwords is also beneficial, alongside using easy tricks to diversify and bolster your password structure.

If users choose to continue with the same password on various platforms, they could easily incorporate the initials or a portion of the platform's name into the password itself.

Q:



Analysis: As expected, most of the users only change passwords when forced to by the platform hosting their accounts, usually in the aftermath of data breaches or as regular precautionary checks. This is followed up by a significant number of users who change it quarterly, followed up by minor portions of users in the other time ranges. A surprising number of users also don't change their passwords at all.

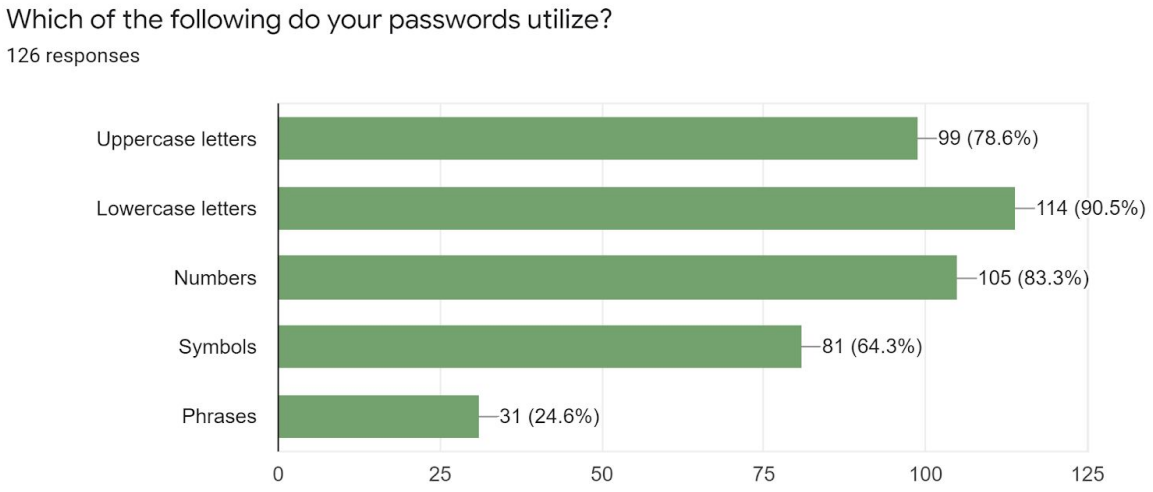
Issue: In some cases, it already gets too late to change the passwords if a data breach has occurred, leading to the compromise of sensitive information. Users who don't change passwords too frequently, or don't change them at all, are the most prone.

Solution: Encouraging users to change passwords on a frequent basis is the key. Using simple methods such as slight alterations to your current password without changing the entire thing has proved to be effective.

SECTION 3

> Password Specific

Q:



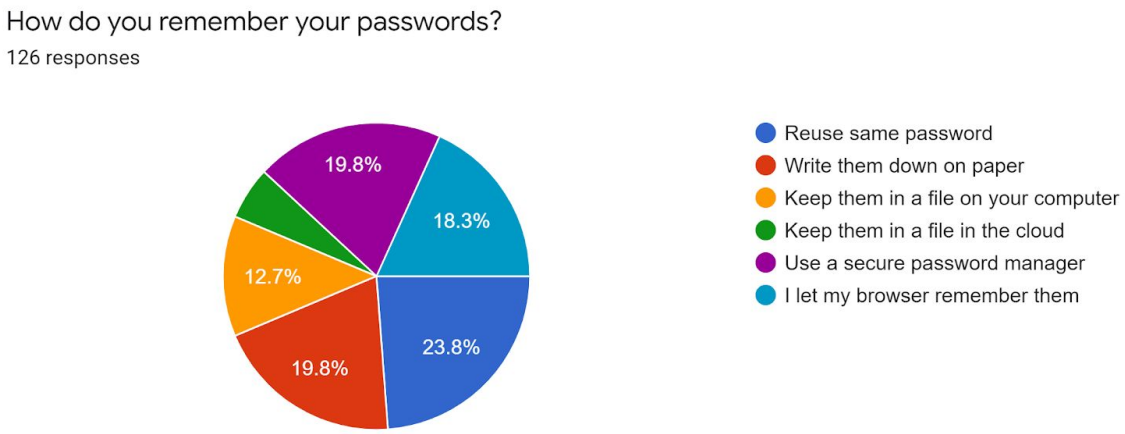
Analysis: While lowercase letters take the obvious lead in the composition of passwords, a satisfactory % of users also utilize a good mixture of numbers and uppercase letters. Symbol usage is something that is highly underrated but provides more scope on the account of password security. Phrases are highly underused, but prove to be the most effective in terms of taking your password and account to new heights of safety. This leads to the establishment of an inverse relationship between increased security and the actual number of users that put in the efforts to make it happen.

Issue: Accounts with linearly structured passwords containing characters from only 1-2 fields/types carry a high risk of being breached. The lack of effort that goes into creating passwords or diversifying them is the major attributing factor here, and easier methods need to be devised to encourage and motivate users to explore better password compositions.
Solution: Platforms now have started to mandate the creation of passwords that are to contain characters from more than one field or type, but this needs to be reinforced everywhere else on a uniform basis. Also, getting deeper into specifics, the usage of phrases can also be made easy. Users could take a memorable phase and incorporate the initials of the line within their password. This inadvertently becomes easier for the user to remember, while hackers will find such passwords as incomprehensible gibberish.

Q: What is the average length of your passwords?
Analysis: Almost 3/4ths of the user pool favor using passwords 8-12 characters long, while 1/5th of the users have passwords exceeding 12 characters that might fortify security in some cases. The remaining take the unsafe route by settling with passwords that have less than 8 characters.
Issue: The problem here lies with the need for longer passwords that are a bit less susceptible to breaches.

Solution: Platforms need to mandate the requirement for longer passwords during account registrations. While the current implementation is quite comprehensive (with password security bar meters being available), more efforts have to be put into making it widespread.

Q:



Analysis: As noticed from earlier, users prefer reusing the same password over and over again, which becomes more convenient for them to remember. People also prefer writing down passwords on a piece of paper, which has its own pros and cons. A large chunk of the users surprisingly uses secure password managers, more than keeping files on the desktop or storing them in the cloud.
Issue: The reuse of passwords once again proves to be the major issue, increasing the chances of account breaches. Organization and storage of passwords have also proved

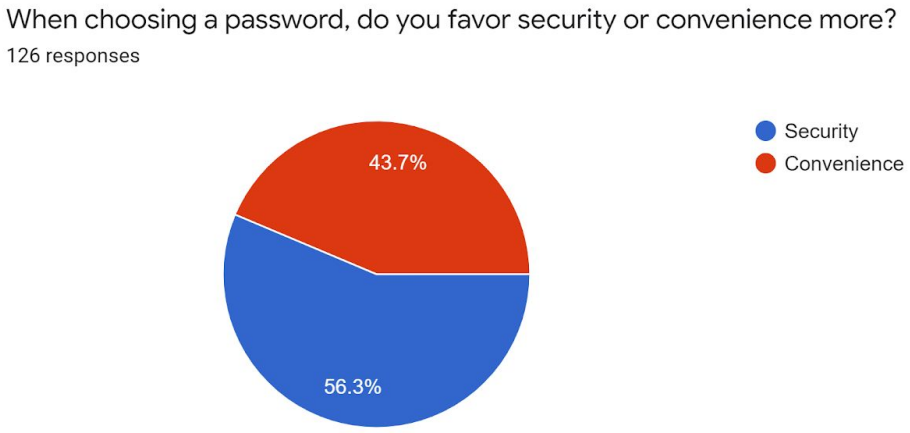
to be a hefty task for many involved, as they scourge around for easier methods which can potentially get their accounts compromised.

Solution: Introduction of user-friendly password managers, motivating users to alter their passwords with minor modifications with respect to the platform being used, and keeping backups of the passwords in the case that the user has forgotten them are some easy solutions to tackle this.

SECTION 4

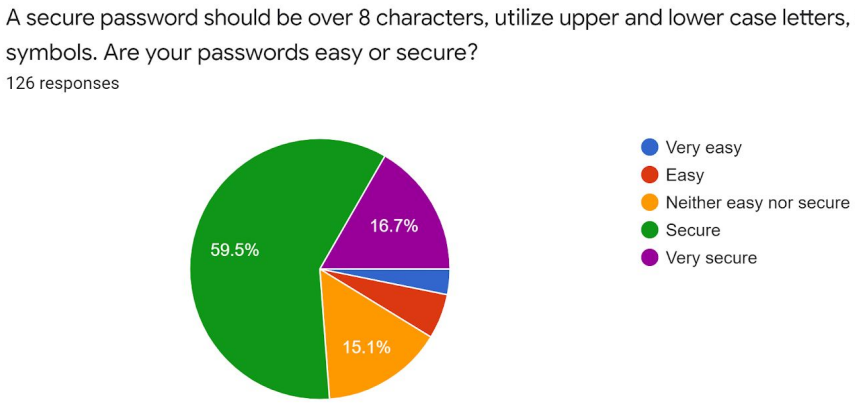
> Mythbusters: Password Edition

Q8:



Analysis: The user pool is almost neck-to-neck, with users surprisingly favoring security over convenience, albeit not with a really substantial difference between the two.
Issue: The personal interpretation of security is what comes into play here. Users often misunderstand the true meaning of security, with the common parameters that they have set for themselves lag behind the actually recommended parameters, attributed to the lack of awareness pertaining to these issues.

Q9:



Analysis: A stupendous 60% of the user pool has already fallen for the misconception. Calling the password which has been based on the given condition ‘safe’, has exposed the common belief that such passwords reach satisfactory safety levels when in reality they actually don’t.
Issue: The casual attitude of netizens over the internet and the minute prevalence of laziness attributes to the fact that they have chosen to craft passwords that meet sub-standard levels instead of opting for more secure ones.

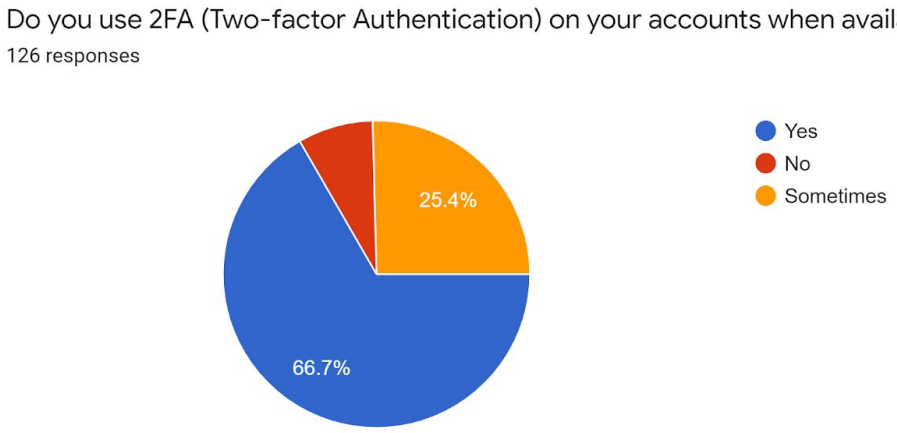
Solution

Once again, such issues and beliefs can only be tackled by spreading awareness on a widespread basis among different age-groups of internet users is key to tackling this issue, and busting such ever-growing myths and misconceptions once and for all.

SECTION 5

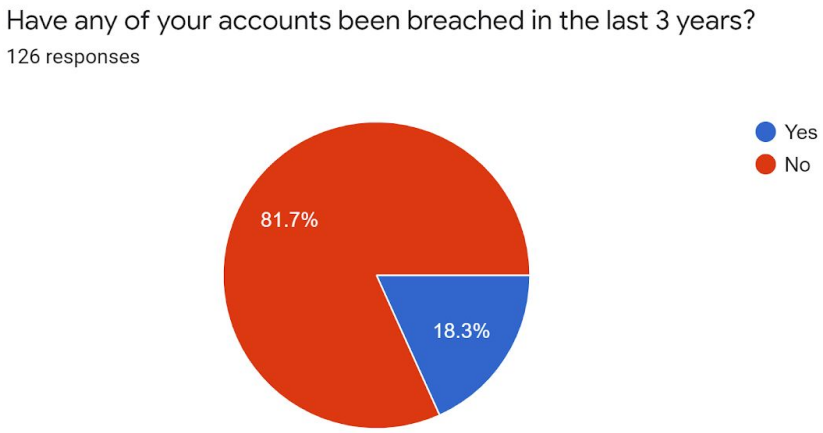
> Miscellaneous and Conclusion

Q:



Analysis: A bit over 2/3rds of the user pool choose to opt for 2FA services, while about 1/4th use them irregularly in some form or the other. Surprisingly, only about 1/10th choose not to opt for 2FA, in stark contrast to the ones who do.
Issue: The complexity of the authentication system can pose issues.
Solution: 2FA services need to be made more flexible and accessible in order to encourage all users to opt for this. It is an excellent, foolproof method and carries a lot of potential

Q:



Analysis: 4:1. The ratio between people who haven't experienced an account breach in the past 3 years, to the people who have. The numbers look positive, but methods need to be devised to increase the overall security and negate the threats of breaches.

Issue: The accumulated misconceptions and errors we have covered so far play major roles in decreased security of accounts and lead to the creation of susceptible and weak passwords.

Solution: Netizens need to act smart, follow protocols and rules they think are best for them and their account safety - by fortifying passwords, managing them efficiently, keeping good and safe conduct online, and reporting any bugs or threats that could potentially compromise their safety.

SNOWFLAKE

THE PASSWORD MANAGER TOOL

Insights

> What is it?

Introducing **Snowflake**, an innovative and organized password generator/manager multi-browser extension that enables users to maintain their passwords, find out descriptive details and statistics going into the password, as well as provide state of the art encrypted suggestions.

> How has it been made?

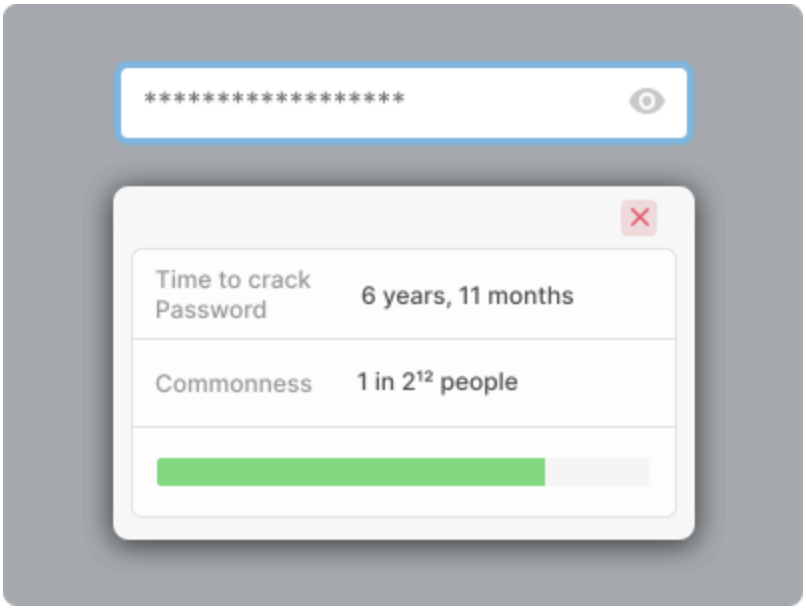
- **Javascript** has been primarily used for building the web application, and for other backend processes.
- We have also used **HTML5** + **CSS3** as the formatting language, for interaction designs and the manager layouts and interfaces.

The website and the project can be accessed through the following link:

https://snowflake-project.github.io/

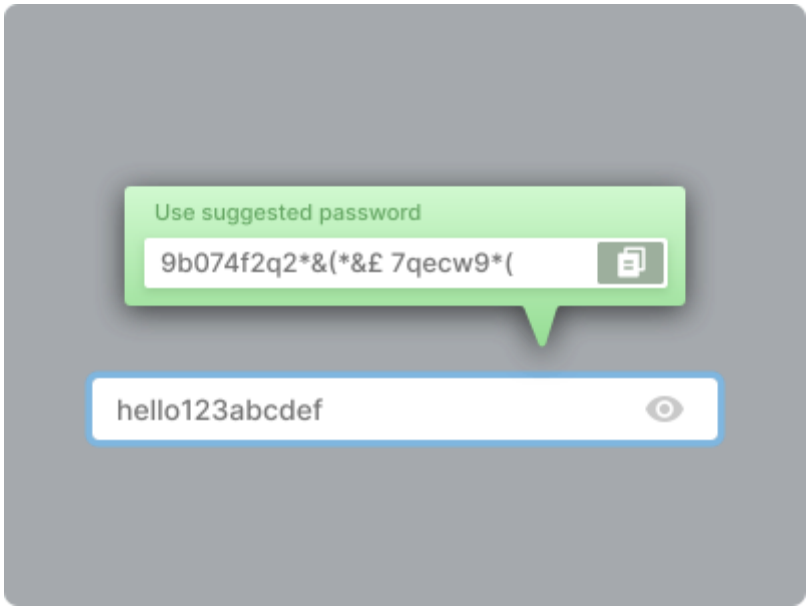
Working and Background

> Features



The manager comes with a descriptive, interactive floating overlay that provides critical statistics and information relevant to the passwords, such as the time it'll take for it to get cracked, along with the commonness of the password.

The sophisticated, state of the art password generator provides users with encrypted and highly-random suggested passwords that greatly enhance their security.



> Our inspiration and purpose

The need for an easy-to-use, interactive and lightweight model that manages passwords of netizens hailing from different backgrounds coupled with the level of experience they possess on the account of internet usage was the main source of our inspiration.

A minimalistic, modernistic take on the overall layout of the manager inspired by current UI/UX trends also helps us to identify the interfaces users prefer, usually, the ones that look the most appealing and are comfortable to work with in its general nature.

Hence combining both reliable and sophisticated programming along with a multitudinous and understandable design layout, we aim to provide users with the best password security and management service out there, to make the internet a safer and more enjoyable platform.

Conclusion

The repercussions of identity theft can be long-lasting and they are not only limited to financial problems. The victim could also face a range of emotional implications, including stress and anxiety. Therefore, it's important that you take measures to protect yourself from the burdens of having an account hacked.

If you want to keep your accounts and personal information safe, it's vital that you understand how to create a strong password. Are you guilty of using '*1234*', '*admin*', or '*password*'? If you are, it's time for you to work on your password security.

Security measures such as passwords are critical when it comes to preventing unauthorized access to one's computer and mobile devices. In today's world, hackers and other cyber-criminals are continuously finding new ways to gain access to these devices in order to steal or exploit the information within. Careless use of passwords, however, can be as bad as leaving one's computing devices unprotected. For this reason, people should create and protect their passwords with care.

Abstract

The purpose of this group research was to establish a direct link between netizens and their knowledge and awareness about password security and management.

In the first phase, we covered general **research** details pertaining to an overview of Cyber Security, along with a deeper look into Password Security and Management - its definition, use, importance, and the methods through which your account can be breached.

Moving to the core component of the report, we provide a detailed and critical analysis of the conducted **survey**, contributed to by over 120+ surveyors, where we tackle each question asked with a constructive format providing insight, bringing out existent issues and myths and on solutions to tackle them.

The final leg of the report covers our password manager **tool**, Snowflake, providing details about its features, languages used, and other miscellaneous information.

The three components are shortly followed up by a comprehensive conclusion.

Bibliography

1) https://digitalguardian.com/blog/what-cyber-security#:~:text=The%20Importance%20of%20Cyber%20Security&text=Organizations%20transmit%20sensitive%20data%20across,to%20process%20or%20store%20it.
2) https://www.highspeedtraining.co.uk/hub/password-security-guidance/
3) https://en.wikipedia.org/wiki/Password_strength
4) https://en.wikipedia.org/wiki/Password_manager
5) https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords
6) https://www.techsafety.org/passwordincreasesecurity

Survey through **Google Forms.**