Password Manager

Project submitted to the

SRM University – AP, Andhra Pradesh

for the partial fulfilment of the requirements to award the degree of

Bachelor of Technology/Master of Technology

In

Computer Science and Engineering

School of Engineering and

Sciences

Submitted by

Yuvaraj Prudhvi Majeti

(AP22110010037)

Under the Guidance of

Mrs. Karnena Kavitha Rani

SRM University–AP

Neerukonda, Mangalagiri,

Andhra Pradesh – 522502

[December - 2023]

Certificate

Date: 10-Dec-2023

This is to certify that the work present in this Project entitled "**Password Manager**" has been carried out by **Yuvaraj Prudhvi Majeti** under my/our supervision. The work is genuine, original, and suitable for submission to the SRM University – AP for the award of Bachelor of Technology/Master of Technology in **School of Engineering and Sciences**.

Supervisor

(Signature)

Prof: Mrs. Karnena Kavitha Rani

Designation: Coding Trainer

Affiliation: CSC

Acknowledgements

Technology is moving fast, and hackers are keeping up. Surprisingly, though, human customs aren't changing quickly. The same tricks that have fooled people for ages are stillwired into our brains. Those same methods are still being used to hack individuals and businesses today. But the good news is, it doesn't have to be that way!

I would like to thank my faculty mentor, my team members and everyone who was involved in this project.

Special thanks to Rachel Tobac for teaching us how to protect our passwords in a secured way. I learnt a lot through her various interviews across all social media platforms.

Thanks to David Bombal for spreading the knowledge of cybersecurity and ways to build our online presence in a healthy manner.

Table of Contents

Abstract

In the fast-paced digital era, where our lives are entwined with multiple online activities, the urgency to prioritize our cybersecurity has never been more critical, especially for young engineering students aged 17-20. This report addresses the common oversight of online security among this demographic, drawing attention to the pervasive threats posed by cybercriminals exploiting our hectic online lifestyles. It vividly portrays the chaotic digital landscape we navigate daily, highlighting how hackers adeptly manipulate our sense of urgency, pushing us into hasty decisions and making us susceptible to scams.

.

The heart of the report delves into the paramount importance of cultivating unique passwords and the transformative role of password managers. By resonating with the students' daily experiences, it underscores the risks associated with password reuse and the potential fallout across personal and professional domains. Introducing LastPass as a tangible example, the report explains how password managers simplify the creation and management of secure passwords, freeing students from the burden of memorization. This section emphasizes the practicality of adopting such tools, especially in the context of the students' busy academic and personal lives.

Recognizing that cybersecurity extends beyond passwords, the report educates engineering students about the necessity of Multi-Factor Authentication (MFA). It elucidates MFA's role in fortifying digital defenses, providing real-world examples familiar to the demographic through popular apps and websites. Additionally, the report introduces the concept of threat modelling, effectively breaking down the likelihood of specific cyberattacks. It concludes by offering actionable advice, urging students to proactively embrace digital security practices such as regular device updates, session management, and the adoption of password managers and security keys. By merging accessibility with urgency, this report aims to empower young engineering minds in India with the knowledge and tools to navigate the digital realm securely.

As people begin their professional journeys, the report also sheds light on the methodologies employed by cybercriminals. By demystifying terms like Open-Source Intelligence, Password Dumps, Phishing, and Social Engineering, it provides a foundational understanding of the techniques threatening their digital lives. The report emphasizes the students' unique threat models, drawing a connection between their online behaviors and the potential risks they face. Tailoring the advice to suit varying threat levels, the report guides students on adopting comprehensive security measures, urging those with heightened threat models, such as those in administrative roles or with a significant online presence, to integrate security keys and multi-factor authentication for enhanced protection. Ultimately, this report serves as a beacon of practical knowledge, equipping young engineering students with the tools to digital landscape with confidence and resilience.

Statement of Contributions

Give below are the responsibilities and contributions of each candidate in this paper.

Coding – Dattatreya Nammina (AP22110010025)

Graphics – Narasimha Rallabandi (AP22110010028)

Research – Yuvaraj Prudhvi Majeti (AP22110010037)

Editing – Akhilesh Vallabhaneni (AP22110011504)

Introduction

We're all busy these days. Most of the time, we've got 3 to 12 browser tabs open, we're using three different apps on our phones, juggling video meetings while dealing with emails, and our calendars are packed, leaving little time even for a quick desk salad.
Hackers are aware of this hectic pace. They skillfully use the idea of urgency to trick people.They pressure their targets to make quick decisions, skipping careful thinking and logical judgment. This leads us to fall for scams. Experienced cyber criminals take advantage of our natural tendency to prioritize immediate action over careful thought. They exploit ourvulnerability in moments of urgency to make us comply with their malicious plans.

Importance of unique passwords and password managers

When people log into their accounts, many tend to use the same password repeatedly or make slight modifications to it. If you've experienced a data breach (which is common for most of us), cybercriminals can take that password and try using it on other sites you frequent—such as your bank, work accounts, and personal email. Reusing passwords is the simplest way to make yourself vulnerable to hacking. Even if it's for sites you consider unimportant or disposable, using the same password across multiple platforms can be risky.Criminals could exploit this by using the password against you. Therefore, it's crucial to create strong and unique passwords for each site. It's highly recommended to store them ina password manager that ensures their safety through encryption and can even generate secure passwords for you.

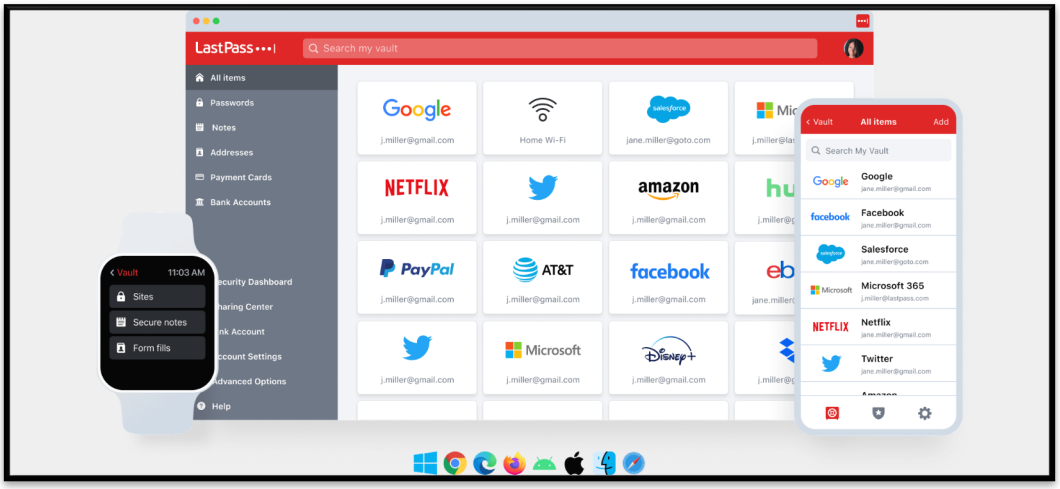

Figure 1: Last Pass

Dealing with numerous complex passwords can be overwhelming. That's where password managers step in. They offer a secure and convenient solution by creating, storing, and automatically filling in strong, unique passwords for different accounts. With a password manager, you can easily maintain secure and distinct passwords without the need tomemorize them (or resorting to writing them on notes, which might end up in the background of Instagram pictures). This significantly lowers the risk of breaches related topasswords. In a corporate setting, embracing unique passwords and password managers isa crucial aspect of a strong cybersecurity strategy. It enhances the protection of sensitive data, secures company resources, and strengthens the overall security stance of the organization.

Multi-factor authentication (MFA) and its significance

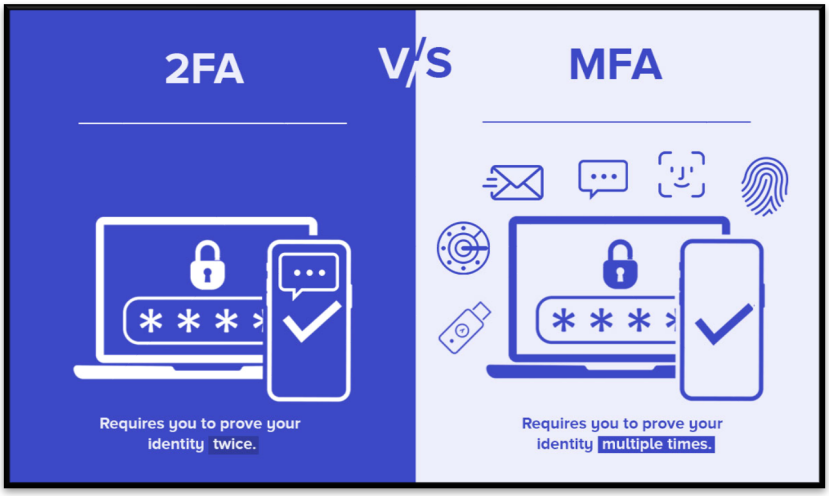

Figure 2: 2FA V/S MFA

Passwords alone are not sufficient for ensuring security. It is essential to utilize strong andunique passwords stored in a password manager, coupled with the implementation of multi- factor authentication (MFA). MFA, a security measure requiring multiple forms of verification, goes beyond traditional username and password combinations. This added layer of protection, incorporating factors like something the user knows (e.g., a password) and something the user has (such as a unique code or token), significantly enhances security.While many are familiar with MFA, understanding its importance is crucial for obtaining team buy-in. The significance of MFA lies in its ability to mitigate risks associated with compromised or weak passwords. Even if a hacker obtains a password, access to theadditional authentication factor is still required, reducing the likelihood of unauthorized access. MFA acts as a defense against various security threats, including phishing attacks andcredential stuffing, by introducing an extra barrier that complicates the impersonation of legitimate users.

Additionally, MFA serves as an early warning system, as any unauthorized attempts to access an account will prompt alerts or necessitate further verification. The implementationof MFA is particularly critical for sensitive accounts or systems holding confidential information, playing a pivotal role in preventing unauthorized access, data breaches, loss of brand trust, and identity theft. By advocating for and ensuring the widespread adoption of MFA within your organization, you can substantially strengthen security measures and safeguard valuable company assets.

Methodology

Cybercriminals make use of various password databases that are available publicly throughvarious data breaches. They will be using various techniques like Open-Source Intelligence,Password Dumps, Phishing, Social Engineering etc.

Threat model is basically the likelihood that you are to receive a certain type of attack. If youthreat model is super high, you are probably a businessman or politician or a big social media influencer. There are many people looking to gain access to your data, money, status etc. People with elevated threat model must be extra secure and careful because they aremore likely to get attacked. People with lower threat models like you don't have admin at work, maybe you are not in a public eye, and you don't use social media frequently. It meansthat your threat model is low. If you are having an elevated threat model, you have admin access, politician etc you must start using multi factor authentication like security keys. If you are not having a threat model just turning on multi factor authentication is going to stop70% of the attacks.

In this digital world to protect yourself from attacks it is important to store a generatea long bit password stored in a password manager. So that there is no need to remember andturn on multi factor authentication, make sure you understand your threat model. But for some reasons people think that they are never going to use a password manager, because they are not comfortable with that digital type of product. They are much more comfortable reusing their passwords across all the sites.

Using of a digital password manager and physical security keys are much more importantfor people who are having a high threat model. Passwords should be kept in such a way thatit takes more time to crack them. It is recommended to have long, random and unique passwords as long as you are comfortable sorted in a password manager. Password manager can just enter it for you or type in all the characters and you don't need to remember anything. If you are still not convinced to use a password manager, then try to add some characters at the end, middle or start to password. Even if the encryption of the password manager encryption is breached which is generally not possible. If in case password manager encryption is breached your password are safe.

If you are even more afraid of attacks, you need to re-login or re-authenticate your sessionsevery half of the day. Even if someone gains access to your machine, they are not a whole theycan do because you are getting logged out. You can also make sure that your cookies are clearing so that your sessions are not there on your browser for a long period of time. As you are using hardware security keys and long random unique password that is extremely safe. When people try to contact you verify that whether it is an authenticate communication.

Make sure all your machines are up to date. If there is a new patch or update on your device,make sure they are updated.

Discussion

Figure 3. Hardware security key

Figure 4. Software Update

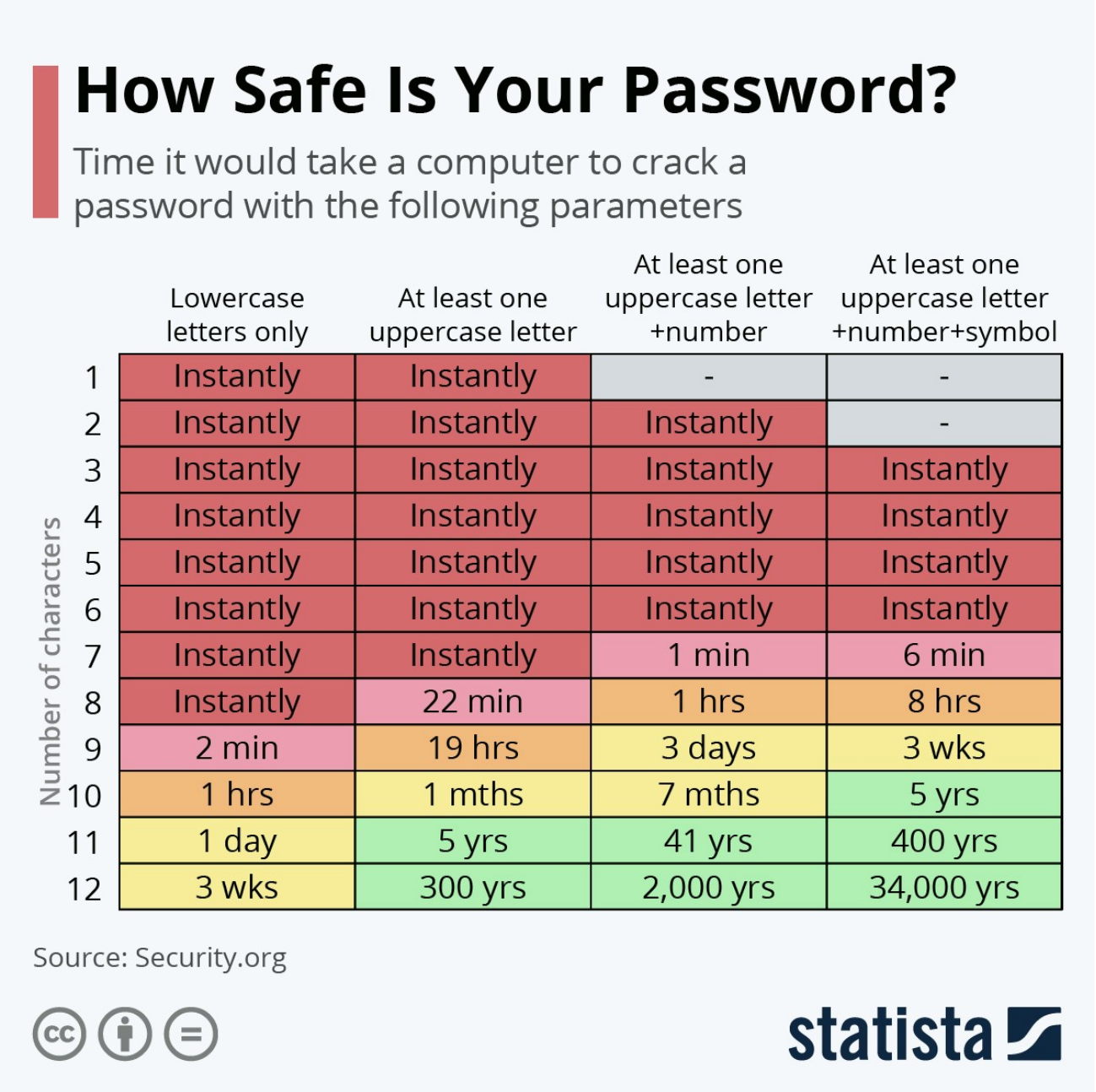

Figure 5. Passwords Crack Time

The above given image shows us the time required to crack a password. So, make sure youuse long, random, and unique passwords for all your online sites. Never try to use the samepasswords across all sites as it may be easy to compromise your accounts.

Concluding Remarks

- Aim of the project is to develop an understanding of password management in this digital world.
- Always pause and think before clicking on links or giving out personal information online. It's like checking who's knocking at your digital door.
- Investigate emails or messages that seem suspicious. If something feels off, don't open it.
- Keep your devices and apps up to date. Updates are like getting coolgadgets for your digital fortress, making it stronger against bad guys.
- Take charge and be the guardian of your digital castle. By being smart online, you make the internet a safer place for everyone!
- Spread the word to friends and family about being cyber-savvy. It'slike creating a team of digital heroes, protecting each other online.
- When you're done playing in your online world, do the logout! Log out from your games and apps, just like saying bye to your digital friends.
- Play nice in the digital playground. Treat others how you want to betreated. It's like making friends in a new game—everyone wins!
- When your apps ask for updates, say yes! It's like getting power-ups for your digital adventure—new features and extra protection!
- Just like keeping your favorite things hidden, keep your passwordsa secret. Don't share them with anyone, not even your digital friends!

References

1. David Bombal Interview with Rachel Tobac – YouTube
2. It was easy to hack a billionaire – YouTube
3. Inside the mind of an ethical hacker – YouTube
4. Modernize MFA with YubiKey – YouTube
5. Hackers Guide to Secure your Organization – eBook
6. Saket Modi on Cybercrime – YouTube
7. O. P. Manocha on Cyber Warfare – YouTube
8. Cyber Encounters: Cops Adventures With Online Criminals – Book
9. Hacked and Helpless? The Power of Reporting – Article