EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 5||pp 1-9||June||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

How to Protect Your Passwords and Secret Personal Notes

Evariste Sibomana[1*]& Papias Niyigena (PhD)[2]
[1,2]Faculty of Computing and Information Sciences, University of Lay Adventists of Kigali (UNILAK)
Corresponding Author Email: bsieva@gmail.com

Accepted: 19 April 2025 || Published: 06 June 2025

Abstract

Many people think of using passwords for their data security, but few of them think about how to protect their passwords. The passwords we use also need to be protected. While creating a password, it's better to create a strong password, but because many people can forget it, they choose to use weak or reused passwords, which make their accounts more vulnerable to breaches. Many people forget their passwords, and sometimes it's impossible for some systems to restore forgotten passwords. This is why I thought the solution of that problem: Creating a writing system (script) as secure method to write and save offline my passwords or/and secret personal notes. The result of this study is to show that anyone can create easily not language, but his own alphabets or writing system (script) and this will help to resolve the problem of forgetfulness and confusion of passwords and you will never have fear again of creating strong passwords or passphrases. The finding will also help to write and save safely your secret personal notes using your own writing system (script).

Keywords: *Password, writing system, Two-Factor Authentication, Multi-Factor Authentication, hacker, cybercriminal*

How to Cite: Sibomana, E., & Niyigena, P. (2025). How to Protect Your Passwords and Secret Personal Notes. *Journal of Information and Technology, 5*(5), 1-9.

1. Introduction

To protect your information, networks, devices… you will need to use a serious authentication process (username/password, biometric). When you are using a password, it's advisable to use a strong and unique password that will be so hard, even impossible, to be cracked by hackers or cybercriminals. Because it's not easy to memorize a strong password, many users choose to use weak or reused passwords.

Because web browsers have the option of saving passwords (Password Manager), many of us use this method frequently, and that leads us to forget our passwords. If you change or lose your device, it will be a big problem; you may lose all of your passwords saved in your web browsers. Saving your passwords in your web browser's Password Manager also may be a serious security risk because if someone gains access to your device, then your passwords can be easily accessed.

When you've forgotten your password, resetting is not always easy for all systems and websites.

For some systems, only the administrator has Super Admin privileges to reset your password, then other users have to send their request and wait the feedback, which can take even long time depending on the availability of support team.

It is so distressful if you want to reset your forgotten password and you're told that:

"Passwords cannot be reset on this site."

"Unable to Reset Password, please contact your system administrator."

"Your account is not enabled for password reset."

For these reasons, it's better to have a secure method of saving your passwords.

To solve all of these issues, I found that it's better to have your handwriting notebook where you keep all your passwords and must be written in your own writing system (script).

In this paper, I'm going to show how it is easy to make your own writing system, which you can use to write and save offline your passwords and your secret personal notes.

1.1 Types of passwords

1. **Alphanumeric Password**: To form this type of password, you can use English alphabets, numbers, and/or special characters.

1. **Passphrases**: To form this type of password, you have to use different phrases. (This type of password is easy to remember compared to Alphanumeric or PIN).
2. **Personal Identification Number (PIN)**: This type of password is not as complex as alphanumeric passwords. Your PIN is securely stored on your device, it isn't transmitted anywhere, and it isn't stored on a server. This makes it more secure than a traditional password.
3. **Biometric Passwords**: Use your iris, fingerprints, or face to enter your accounts.
4. **Pattern-Based Passwords**: It is a simple method of authentication by drawing a simple pattern on the screen of your device.
5. **One-Time Passwords (OTP)**: It is a dynamic and synchronized password that is valid for only one login session or transaction on a computer system or other digital device. This type of password is also generated automatically for multi-factor authentication (MFA), or Two-Factor Authentication (2FA).

In this research, we encourage that these first three types of passwords may be written and saved offline by using your personal writing system (script).

1.2 Problem Statement

While there is no limitation on creating different accounts which require unique usernames and passwords, the issue of forgetting or confusing them becomes more complex and may sometimes cause the problem of losing created accounts and their contents. Some systems use encryption to hide and protect passwords, but that can't be the solution to the problem of forgetfulness and security of the passwords. Some people choose to create very easy or reused passwords so that they will never forget them, but that will help hackers or cybercriminals to penetrate their accounts. Using a Password Manager also increases the problem of forgetfulness of the passwords and can be a serious security risk because if someone gains access to your

device, they can easily access all of your saved passwords. Creating a strong password, which is better and advisable in data security, is sometimes ignored because memorizing it is so difficult, especially when you have many different passwords for various accounts.

1.3 Purpose of Study

The main purpose of this research is to show that anyone can have his own personal writing system (script) which can be used to write and save offline their passwords and secret personal notes.

1.4 Objectives

The specific objectives are as follows:

i. To solve the problem of forgetting or confusing your passwords.
ii. To show that you can protect your accounts' usernames and passwords effectively.
iii. To show an easy method of creating your personal writing system (script).
iv. To protect your secret personal notes.

2. Literature Review

A survey done by iProov and published on their website shows that: "forgotten passwords are a global problem impacting consumers and businesses." (iProov, 2021).

57% of Spanish and 54% of Americans say that they have abandoned an online purchase or online booking because they had forgotten their password, and retrieving it took too long. (idem).

According to Verizon's 2024 Data Breach Investigations Report (DBIR), attacker gains access via hacking by the Use of stolen credentials (77%), Brute force (usually easily guessable passwords) (21%), or an Exploit vulnerability action (13%) (Verizon, 2024).

Forbes shows that 38% of users make mistakes by writing down their passwords, 32% use the same password across multiple accounts, and 24% store their passwords on their computers

(Forbes, 2024).

According to the survey from TechRadar and OnePulse, over 60% of the respondents said they reuse the same password across multiple accounts. The reasons remain the same, as 40 percent don't want to remember multiple passwords, and 27% said that they don't think they're in danger of being hacked, so using unique passwords seems like a waste of time (Bitdefender, 2022).

It is extremely common to forget a password, with 78% of people having to reset at least one password every 90 days because they forgot it. In fact, 21% of people forget a password after only two weeks of creating it (zippia.com, 2023).

More than 80% of confirmed breaches are related to stolen, weak, or reused passwords (Norton, 2021)

More than 6 in 10 people admit to reusing passwords (Norton, 2022).

96% of the most common passwords can be cracked by hacking tools in less than one second (Norton, 2022).

1 in 4 internet users save their passwords in their web browser (Security.org, 2023).

Roughly 3 in 10 employees create strong passwords for their work accounts (Norton, 2022).

45 million people rely on password managers to keep track of their passwords (Security.org, 2023).

According to jumpcloud.com, 70% of weak passwords can be cracked in less than 1 second by hackers using simple brute force attacks (jumpcloud.com, 2024).

Multi-Factor authentication (MFA), or Two-Factor Authentication (2FA), makes you 99% less likely to be hacked (Lucas Augusto Meyer, Sergio Romero, Gabriele Bertoli, Tom Burt, Alex Weinert and Juan Lavista Ferres, 2023).

2FA is not 100% hacker-proof; it significantly increases security, but can still be vulnerable to sophisticated phishing attacks and other methods. One such method is called SIM-swapping, where a hacker transfers the SIM of a user's device to their own mobile device via social engineering methods (Timus, 2024).

Yet despite most people receiving some cybersecurity education, our report found that many (62%) are still reusing passwords. Why is that? It turns out that education and awareness might not be enough (Norton, 2022).

2.1 Best way to store your password:

Your password is supposed to protect your important data, but it must remain a secret.

Storing passwords offline is important because your password is not as safe as you think it is. Each year, 7 to 10 percent of Americans are victims of identity theft. A total of 21 percent of these people are repeat victims. (CLEVER FOX).

Many data breaches happen because of insecure passwords, so it is important to keep passwords safe if you want to protect your personal information.

When storing passwords offline, a paper password book is the best option. Because pen and paper cannot be hacked, they can keep your passwords safe for years to come. The best way to remember your password is to write it by hand. (CLEVER FOX).

2.2 Characteristics of best password:

1. A password must be unique: every account must have its own password.
2. A password must be random: Make sure that your password doesn't contain any of your personal information, and mix lowercase and uppercase letters, numbers, and special characters.
3. A password must be long in size: A password with 8 characters will take from a few seconds to a couple of hours to crack, while a 16-character password will take a hacker a billion years to crack. Never use a password less than 14 characters.

Anyone can use Password strength testing online tool to evaluate the strength of his password by using this link: https://bitwarden.com/password-strength/

3. Methodology

In this research, we have used qualitative research methodologies.

Qualitative research is a methodology that uses non-numerical data to better explore the motivations, responses, and experiences of people.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 5||pp 1-9||June||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

4. Findings and Discussion

In this research, I have converted English alphabets (uppercase and lowercase) and decimal numbers into my personal writing system (called **Sieva's writing system**), but ignore special characters and symbols.

Bloomfield opined that "writing is not language, but merely a way of recording language by means of visible marks" (Bloomfield 1933, p. 21).

I'm going to show you how it is easy to create your own writing system (script) and use it to write and save your passwords in your note book and none except you will read it.

Your writing system must be unique and personal.

Every alphabet and number has to be converted one by one, and every converted alphabet must be unique and easy to write than its original alphabet, and this will help to memorize easily all converted alphabets.

I'm not going to give you all my converted alphabets, it's my own personal writing system (script) used since 1999, and all of my secret information are written in that way, but I'm going to show you how is easy to make your own by taking some characters by default.

Converting alphabets (uppercase):

A=

T=

W=

Converting alphabets (lowercase)

a=

t=

w=

Converting numbers:

0=

1=

7=

You can also change some of special characters and symbols into your writing system, but in this paper, we continue using them without conversion.

Below is an example of writing a strong password in my writing system style:

This password is composed of letters (uppercase and lowercase), numbers, and special characters and has a length of 18characters, and myself can read this password.

I can write all of my usernames and passwords in my notebook and none will read them; this will prevent the problem of forgetting or confusing passwords when you have many accounts.

4.1 Characteristics of good personal writing system:

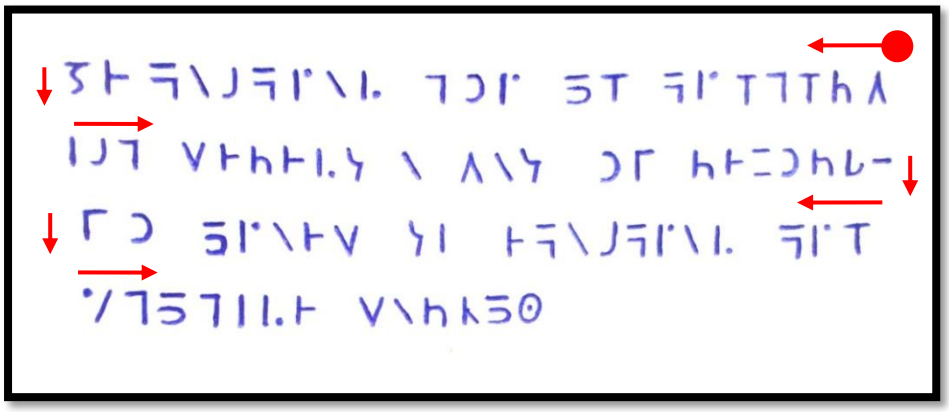
- Easy to write and read;
- Impossible to decipher;
- No similarity between converted character and its origin character;
- No duplicates between lowercase and uppercase characters.

4.2 Writing directions:

There are many writing directions, and you have to choose which one you will use in your writing system. (Omniglot, 2024).

Some Examples of writing directions:

- Boustrophedon: (alternating direction right to left then left to right),

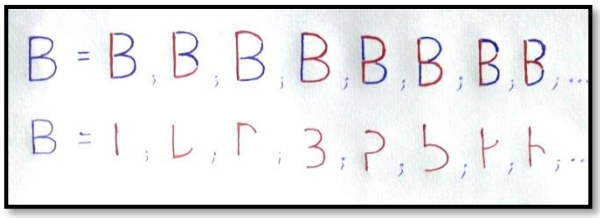


- Left to right, horizontal (used by many people when writing Roman alphabet),
- Right to left, horizontal (used by writing Hebrew, Arabic …),
- Top to bottom, horizontal (Used for East Asian languages:),
- etc.

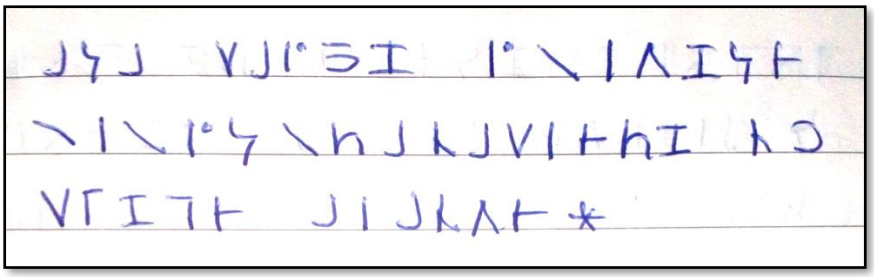
For more information about how to create your own writing system (script), you may read the guidelines on https://neography.info/create-a-script/#step-2

4.3 Possibilities of creating your own script

There are many possibilities of making your own script, but here are some of them which are very easy, but you can also invent your own script as you want.



Below is an example of my personal notes recorded using my own script.



It's very easy! You can make your own script.

5. Conclusion

Creating your own writing system (script) will be a perfect method of writing, protecting, and remembering your passwords and personal notes. The best secure method to use for remembering your password, even strong password is to have your personal writing system (script) and make a password or passphrases greater than 14 characters (mixing uppercase, lowercase, numbers and special characters), then lastly use Multi-Factor Authentication (MFA), or Two-factor Authentication (2FA). You can use FontForge application to draw your own characters (letters), and you can get your free FontForge app online.

6. Recommendations

Never use a password notebook if you don't record your secret in your personal writing system.

Take a picture of your handwriting password recorded using your own writing system, then save it on your machine, phone, or email so that you can get it easily. Never share your password using social media unless you're using a personal writing system, and never use a weak or reused password. If you save your passwords in your web browser password manager, please secure your device with a password, and never leave it open, because someone may steal your password through password manager.

Acknowledgements

I would like to thank my best Friend Jesus Christ for his grace which grants us life and wisdom.

My gratitude also goes deeply to the family of KARANGWA Jean Népomuscène (PhD) for its great contribution and support. I can't forget to thank my lovely darling UMULINGA Eleda, my uncle Mr CYUBAHIRO Louis and family of MUGISHA Amos for their encouragement and support. Special thanks to my supervisor NIYIGENA Papias (PhD) for your prime contribution, and Mr. MTATIRO Senseri for taking your time to review and make comments and suggestions on the draft of this paper. There are many other people who are not named here but who contributed to this work, may Almighty God bless you all.

References

[1] Kebede Gedefaw Abie, Kenefergib Asefa (2019). THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES.*An Error Analysis of English Paragraphs Written by First Year DebreMarkos College Teacher Education Students: A Discourse Analysis Perspective, Ethiopia,*2.

[2] Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri (2017). An Introduction to Information Security. *Computer security, 77.*

[3] Verizon (2023). 2023 Data BreachInvestigations Report, 43.
[4] LastPass (2022). 2022 Psychology of Passwords report, 2.
[5] Lucas Augusto Meyer, Sergio Romero, Gabriele Bertoli, Tom Burt, Alex Weinert, and Juan Lavista Ferres (2023). HOW EFFECTIVE IS MULTIFACTOR AUTHENTICATION AT DETERRING CYBERATTACKS? 1,4.
[6] Amit Singha Roy (2021). How to keep your password secure in 2021. *Some tips to keep your password secure*, 2-6.
[7] Geeksforgeeks (2024). Types of Password, accessed on 14th/2/2025. https://www.geeksforgeeks.org/types-of-password/
[8] Zippia (2023). 20+ TELLING PASSWORD STATISTICS [2022]: WHY YOU SHOULD CHANGE YOUR PASSWORD HABITS accessed on 14th/2/2025. https://www.zippia.com/advice/password-statistics/#:~:text=78%25%20of%20people%20have%20reset,reset%20at%20least%20one%20password.
[9] Cleverfoxplanner (2025). THE BEST WAYS TO STORE PASSWORDS SAFELY TO AVOID A HACK, accessed on 14th/2/2025. https://cleverfoxplanner.com/blogs/articles/the-best-ways-to-store-passwords-safely-to-avoid-a-hack#:~:text=If%20you%20prefer%20convenience%20over,safe%20for%20years%20to%20come.
[10] jumpcloud (2024). 50+ Password Statistics & Trends to Know in 2024, accessed on 13th/02/2025. https://jumpcloud.com/blog/password-statistics-trends#:~:text=Weak%20passwords%20are%20the%20cause,or%20falling%20for%20phishing%20scams.
[11] National Cyber Security Centre, Top tips for staying secure online, accessed on 25th/2/2025. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
[12] UC SANTA CRUZ, INFORMATION TECHNOLOGY SERVICES, Protect Passwords, accessed on 25th/2/2025. https://its.ucsc.edu/security/passwords.html
[13] Omniglot (2024). Writing direction index, accessed on 25th/2/2025. https://www.omniglot.com/writing/direction.htm#variable
[14] The CBB (2015). How to design your own script, visited on 19th/3/2025. https://cbbforum.com/viewtopic.php?f=31&t=4502
[15] iProov (2021). Forgotten Passwords are Increasing Your Website's Abandonment Rate, accessed on 20th/2/2025. https://www.iproov.com/blog/forgotten-passwords-increasing-websites-abandonment-rate

[16] Timus (2024). Understanding Two-Factor Authentication (2FA) and Its Importance for Enhancing Security. *Is 2FA 100% hacker-proof?* Accessed on 10th/3/2025.

https://www.timusnetworks.com/understanding-two-factor-authentication-2fa-and-its-importance-for-enhancing-security/#:~:text=No%2C%202FA%20is%20not%20100,device%20via%20social%20engineering%20methods.

[17] Norton (2023). Top password statistics to know, accessed on 28th/2/2025.

https://us.norton.com/blog/privacy/password-statistics

[18] Forbes (2024). America's Password Habits: 46% Report Having their Password Stolen Over the Last Year, Top Password Mistakes People are Making in 2024, accessed on 20th/03/2025.

https://www.forbes.com/advisor/business/software/american-password-habits/

[19] Bitdefender (2022). Majority of People Reuse the Same Password on Multiple Accounts, Research Finds, accessed on 15th/03/2025.

https://www.bitdefender.com/en-us/blog/hotforsecurity/majority-of-people-reuse-the-same-password-on-multiple-accounts-research-finds

[20] Neography.info, How to Create a Script, visited on 16th/3/2025.

https://neography.info/how-to-create-a-script/