

Cybersecurity Fundamentals

Lecture 7: Password Management

CYB 670
Cybersecurity Fundamentals

Presented by
Dr. Mohammad Alkhatib

Outline

Password Management

Introduction

Basics of
Password

Effective Tips on
Password
Management

Creating and
Managing Secure
Passwords

Password
Manager Tools

Introduction

- According to the information published in Symantec Norton report, there were more than 34% of the people in 2017 who suffered losses due to password hacking.
- The total cost of hacking was about \$172 billion, which impacted more than 978 million people worldwide with an average loss of about \$142 per user.
- The major components of this entire loss in 2017 included virus infection (53%), scam purchases (33%), and personal financial frauds (32%).
- The email phishing was also one the major component in this fraud of stealing the personal information and account passwords.
- This report also found that more than **20% of the users use the same password on multiple accounts**, which is considered to be very dangerous practice for personal account security.
- And more than 58% of the users have shared their password with other people for once at least.



Introduction

- The ratio of the users of the **finger print passwords** was about 44% and those who use the **patterns** as security measure were about 22% of the people surveyed in the report.
- A large number of users – more than 70% don't follow the password management's standard guidelines and recommendations, which is a big gray area for the online users exploited by the malicious cyber criminals.
- This gray area is badly exploited by the hackers to hack on the accounts, personal information, digital access, and many other cybercrimes.



Introduction

- This trend of not following the standard guidelines in the **millennial** users is much higher than the older users.
- In the light of these startling statistics, it is very imperative that the basics of password management should be adopted in all level of users across the globe irrespective of their nature of internet use.
- The **failure** to adhere with the basics of the password management may result in huge losses to the internet users in all parts of the world.
- **The password management** is very critical in avoiding password theft and subsequently the DoS attacks as well as other cybercrimes



Introduction



Major Topics

- Basics of Passwords
- Effective Password Management Tips
- Creating & Managing Secure Passwords
- Password Manager Tools

Basics of Passwords

- The **basic objective of using a password** is to authenticate your authority to access certain resources.
- The technique of code word to verify a certain authenticity of person, event, or any other activity was used between the two communicators in the old ages.
- The concept of password can be divided into terms of two major eras – the traditional era and digital era.
- From that point, the password evolved to code-words, and then to hard keys and tokens.
- The physical passwords were also introduced in the locks to get access to certain physical resources. This evolution of password continued in different forms and formats in the traditional era of physical world.



Basics of Passwords

- With the advent of modern digital era, the use of password changes drastically in terms of their shapes, sizes and the ways of using them. The use of password in the digital era, especially in the computing field was introduced in 1961 at the Massachusetts Institute of Technology (MIT).
- This time-domain based password first ever in the digital history was introduced as the Compatible Time-Sharing System (CTSS) project, which allowed the multiple users to use the computer power at different time slots. This system was a UNIX operating system-based project.
- From that point of time the **digital** or **cyber password** has evolved to a very complex and comprehensive security level.
- The present forms of the passwords are very strong, reliable, and sophisticated.
- The modern passwords are used for restricting the unauthorized access to the computing machines like PCs, tablets, mobiles, routers, switches, and many other configurable devices.
- Moreover, passwords are also used to access the online digital services connected through internet.



Basics of Passwords

There **different types and forms of passwords** used in the modern world; the following are a few among them.

- Conventional password
- Biometric Passwords
- Two-Factor Authentication
- Multi-Factor Authentication
- Social Media Logins
- Email Logins
- One-Time Password (OTP)
- Smart Keys and Physical Tokens



Basics of Passwords

- The **modern passwords** consist of minimum length of 8 characters and maximum of 64 characters in certain cases.
- The **strength of password** increases with the number of characters because the possibility of guessing and decoding the hash through computer power will be near to impossible in case of strong 64-character passwords.
- Let's expand upon the more aspects of a modern digital password used in the field of computer and information technology such as:
 - **Threats to Passwords**
 - **Good and Bad About Passwords**
 - **How Does Bad Guys Hack Your Password?**



Basics of Passwords

❖ *Threats to Passwords...*

- The major threat to your password is the user sluggishness, which stops the user from following the password management guidelines. The password theft is one of the major reasons of the distributed denial of service attacks and many other data theft, and financial frauds.
- According to the latest research conducted in 2018 finds out that **a large number of the people use very generic passwords like 123456, 12345678, abc123**, and so on. These passwords are very easy to guess and snoop while you input the password.



Basics of Passwords

❖ *Threats to Passwords...*

The major threats to the password theft include:

- Eavesdropping
- Guessing of password
- Cracking passwords through computing software
- Offline cracking of hashes
- Password recovery or reset cyber attack techniques
- Same password use on multiple
- Using default passwords of the system
- Malicious software on your computer like sniffers and keyloggers
- Backdoor exploit
- Malicious plugins
- Phishing
- And others

How to avoid from these threats? You can make your passwords secure and safe by following the standard guidelines and recommended software tools to make your software secure from external and internal threats.

Basics of Passwords

❖ *Good and Bad About Passwords...*

- People are more careless and lazier about remembering hard and strong password; so, they prefer to use simple and easy to remember passwords. That is not a good idea about a good password.
- A **good password** should have the following features:
 - Should be longer in a range of 10 to 15 characters
 - Should not include any plain text, which is easy to guess
 - Should include the combination of the lower and upper-case characters
 - Should include at least one or more special symbols/characters at random place
 - Should include at least one or more numbers at different places
 - Never use your personal information, which is easy to guess
 - Don't ever share your password with others
 - Always change the password pattern
 - Always change your password regularly

If you follow these instructions, you will remain more protected and secure in this highly risky environment of internet.



Basics of Passwords

❖ *Good and Bad About Passwords...*

Now, let's figure out the main points of **a bad password**:

- Plain text passwords
- Short passwords
- No combination of different types of characters
- No use of upper and lower cases randomly
- Reusing of the same password
- Using meaningful words
- Using meaningful word and adding just one digit like “mango1”
- Reusing the same word twice in the password like “fishfish1”
- Using a word in reverse order like “elppa” for apple
- Using garble word like “0” for o and “3” for E and so on; example includes (z3r0)
- Using the same passwords as their usernames or computer account name and similar
 - All of the above mistakes should never be made while choosing a password.
 - Those mistakes can lead you to hacking of your account by different means.



Basics of Passwords

❖ *How Bad Guys Hack Your Password?...*

The cyber criminals are highly skilled and qualified people with negative thinking so they are very creative thinker in devising strategies and methods to steal the usernames and passwords of the genuine users. They can use any new and innovative technology to get hold on your password, but a few very important techniques are explained below:

- **Over the Shoulder Technique:** This is a traditional way to steal any critical information like password. The bad guys try to steal your password when you enter it into the system or online service. This technique is also useful when you write your password on some diary or paper. The hackers try to peep over to see your passwords in different forms in this method.

Basics of Passwords

❖ *How Bad Guys Hack Your Password?...*

- **Dictionary Hacking Technique:** In this form of exploitation, the hackers try to use the words available in the dictionaries of different major languages. They use different combinations and roots with the help of certain software tools to crack the passwords of the users. This is more sophisticated and effective method to hack the passwords.
- **Password Guessing Technique:** This is one of the traditional forms of password guessing. The hackers make guesses to crack the passwords. Those guesses are influenced by psychology, gender, mental approach, background and other factors of the user. Many studies suggest that a majority of the passwords used by the female users include the names of their children, husband, or boyfriends. The hackers take advantage of this trend in women to hack their passwords.



Basics of Passwords

❖ *How Bad Guys Hack Your Password?...*

- **Brute Force Attack Technique:** As you heard about the crypto currency mining by using the computer processor to decrypt the transaction and verify it. The similar types of technique can also be employed by the hackers to guess your password through a password guessing software. This software uses the combinations of different options and words to guess the password. A simple Pentium 100 computer is able to process more than 20 thousand combinations in just one second. So, you can easily understand that how dangerous this technique can be in modern technological environment.

The modern hackers are very creative, experienced, and skilled. They can use an out of the box idea to crack the passwords at any time. So, always take care of your passwords to maintain their sanctity and integrity.

Effective Password Management Tips

- An **effective password management** plays a vital role maintaining higher level of security at work as well as at home.
- **Password management** is the combination of the procedures and activities that should be accomplished on a regular basis as set forth by the security manager, security management agencies, and industry guidelines.
- The number of identity theft in 2017 increased by over one million as compared to the identity theft figures in 2016.
- One user becomes victim of the identity theft in every two seconds in our present connected environment.
- After creating a strong password, a user has to take different steps to maintain the power and effectiveness of the password.
- That means, **creating a strong password is not sufficient for maintaining a strong cyber security**.



Effective Password Management Tips

- You will have to keep a close look at the security and effectiveness of the password after you created a strong password.
- You should take the below-mentioned steps and follow the **guidelines set forth by the security experts and industry standards** to maintain the effectiveness of your system and online accounts.
 - Always choose longer passwords ranging from 12 to 20 or even more characters
 - Password is a completely private property; so, don't share it with anybody
 - Never create same password for multiple accounts or services
 - Never write down your password on paper or copy
 - Never save your password on your computer
 - Change your password after 3 to 4 months
 - Always use different patterns for every password so that it cannot be easily cracked



Effective Password Management Tips

- Never use single number at the end of the password
- Try to use biometric password if available
- Consider using the 2-factor authentication
- Always enable multi-factor authentication on your account if supported
- Encrypt the files and data that contain password related information
- Don't save your **critical passwords** on browsers
- Always try to use a good password manager for managing your password more effectively and efficiently
- Always type your password fast so that no one can guess it
- Always remember password so that you don't refer to any paper or file for the same
- Try to generate strong passwords with the help of password generating software



Effective Password Management Tips

- Never reuse the password over and over again after changing it
 - Never send or save your password in emails because they are not fully secure
 - Always take note of surroundings when you input your password
 - Always choose the strong passwords but those passwords should be easy to remember for you
-
- If you take care of all of the above-mentioned tips, you would remain fully protected from the identity theft and other hacking activities.
 - Thus, you would be able to manage your passwords more effectively and efficiently.



Creating & Managing Secure Passwords



- In the present-day online environment, our business as well as our social life is highly dependent on the computers, internet, software applications, and online services.
- We use username and passwords for accessing those services and resources of the computer devices.
- **Passwords** are very critical and valuable for every online user because our personal, business, social, and many other types of data and information are directly linked with the online services and internet.
- If any **hacker gets hold on our password**, we will become so exposed to many types of losses incurred by the breach of data integrity, privacy, and availability of digital resources.

Creating & Managing Secure Passwords



- So, the passwords are the lifeline of our online existence.
- If our passwords are compromised, we will lose control over our valuable digital assets.
- The **hackers** and **cyber criminals** are becoming so advanced and use the latest, high-tech, and sophisticated techniques to carry out cyberattacks.
- The **password theft** is one of the major objectives of the cyber criminals to inflict serious damage to the common users as well as to the businesses and government organizations.
- The **solution** to this problem is the use of strong password and allied services so that the chances of your passwords to have been compromised are reduced.

Creating & Managing Secure Passwords

Among such **complementary** measures to make your password even more reliable, strong, and effective a few are explained below:



- **Strong Password**
- **Use of Biometrics**
- **Two-Factor Authentication**
- **Multi-Factor Authentication**
- **One-Time Password (OTP)**
- **Using Password Managers**

Creating & Managing Secure Passwords

❖ Strong Password ...

- The first step towards having a secure and reliable password is to create a very strong password.
- The qualities and features of a strong password include:
 - Non-guessable
 - Longer length
 - Complex pattern of characters
 - Complex combination of characters
 - Based on the out of the box ideas
 - Not influenced with the personal behaviors and information
 - Better password management



Creating & Managing Secure Passwords

❖ Strong Password ...

- The first step towards having a secure and reliable password is to create a very strong password.
- The qualities and features of a strong password include:
 - Non-guessable
 - Longer length
 - Complex pattern of characters
 - Complex combination of characters
 - Based on the out of the box ideas
 - Not influenced with the personal behaviors and information
 - Better password management



Creating & Managing Secure Passwords

❖ Strong Password ...

- You can use a **creative idea or expression** and then choose random characters from that idea or expression.
- For example, you think that working in a government organization is so boring. Then you can make an **expression** like 'I get bored with a government job'.
- This expression will provide you clue on how to remember your password. Then you can choose letters, numbers, and symbols from this expression to create a strong password.
- For example, you take "I", "ge", "bo", "w", "a", "gv", and "j" characters from the above expression.
- Now you organize them in such a way that they create a strong password.
- Let's reduce this expression to "Ig3b0W@gV!" to form a strong password.
- Now, what you have to remember is that you used zero instead of "o", 3 instead of "e", @ instead of "a", and '!' instead of "j".
- The capital letters were chosen randomly to make the password even stronger.
- Thus, you created a very strong password with an innovative expression that only you know about.
- It will become very easy for you to remember because you linked your expression and the characters that you chose with certain situations and symbols.



Creating & Managing Secure Passwords

❖ Use of Biometrics ...

- The use of **biometrics** is becoming a new standard for the passwords.
- There are many security experts and security companies that advocate the replacement of traditional passwords with the biometric passwords.
- The **use of biometrics** makes your passwords more secure and reliable.
- Because this is one of the most powerful technologies that scans the uniqueness of thumb impression or other body organs like facial contour, retina of eyes and body gestures.
- As we known the fingerprints are unique in the world; therefore, there would be no alternative of the figure prints.
- Meanwhile, the facial recognition is another important aspect of biometric identification.



Creating & Managing Secure Passwords

❖ Use of Biometrics ...

- With the advancement in the artificial intelligence in the software development, the facial recognition is becoming another important standard for the biometric access to the devices and applications.
- Patterns
- body gestures
- body movement
- shapes of body parts
- body odors
- complete hand scans: has become one of the most important identification standards for the governments in passports, immigration and other governmental procedures.



Creating & Managing Secure Passwords

■ Two-Factor Authentication ...

- The traditional form of authentication is single factor authentication in which you enter your password against your username to access the authorized resources.
- This method is considered as the low secure nowadays due to many reasons.
- One of the main reasons for the **low security** of **single factor authentication** is that it is easy to be compromised if you have to use your password many times a day.
- The single layer security is not powered by any additional layer that means if your password is compromised, you will lose the control over your resources and unauthorized cyber criminals can easily break into your resources.



Creating & Managing Secure Passwords

■ Two-Factor Authentication ...

- The **solution** to this problem is the two-factor authentication and multi-factor authentication.
- The **two-factor authentication** is also known as **dual-factor** and **two-step authentication**.
- In this process, you get one additional layer of security to access your resources.
- When you enter username and password, you will be prompted to enter the pass-code.
- The **pass-code** is normally sent through a text message or automated call on your mobile phone.
- The **pass-code** is normally an auto-generated unique code by the designated server.
- It is only **one time use code**.
- That code is also **time sensitive** which means the code expires after certain time.
- This way your code cannot be compromised by any malicious user.



Creating & Managing Secure Passwords

■ Two-Factor Authentication ...

- In the latest pass-code generating technology, codes can be generated and sent out through emails, text, automated call, web links and other ways.
- In two-factor authentication facial expression, biometric input or other body gestures can also be used.
- Thus, the access to your resources becomes highly secure and uncompromised by adopting two-factor authentication.

The following steps involve in **enabling the two-factor authentication**:

- Add your mobile number and alternate phone number
- Choose the way you want to receive the pass code – either automated voice call or text message
- The test verification code is sent by server to your phone number
- The code is inserted into the field to verify the same
- Two-factor authentication is enabled now



Creating & Managing Secure Passwords

❖ Multi-Factor Authentication ...

- The two-factor authentication improves the security of resource access, but still the level of security that a critical data needs is not sufficient yet.
- There have been found some important issues with the security of the two-factor authentication.
- For example, the RAS security company announced in 2011 that a huge number of important two-factor accounts have been compromised.
- In that attack the Secure ID authentication tokens were hacked by the cyber criminals.

Multi factor authentication



Multi-factor authentication is based on three or more factors. **The major 3 factors used are known as:**

- What you know?
- What you are?
- What you have?

Creating & Managing Secure Passwords

❖ Multi-Factor Authentication ...

Multi factor authentication



❑ What You Know?

- This category of the multi-factor authentication deals with the information or factors that a user knows about.
- For example, password, pin code, or other security code either provided by the service provider company or created by the user.
- This category of authentication factors is also known as the knowledge factors in the field of computer security.

Creating & Managing Secure Passwords

❖ Multi-Factor Authentication ...

Multi factor authentication



❑ What You Are?

- This category consists of the factors that relate to the personal information like facial recognition, biometrics, retina scan, and other factors.
- These factors are also classified as the inheritance factors in some books and technical writings.
- These are very unique biological characteristics or factors for every individual person.
- Thus, it makes the multi-factor authentication more robust.

Creating & Managing Secure Passwords

❖ Multi-Factor Authentication ...

Multi factor authentication



❑ What You Have?

- This group of factors is also referred to as possession factors in the field of computer security.
- In this category, the major factors of authentication include the components like key fob, digital key, or mobile device with the software application to scan.
- These factors are extensively used in the modern multi-factor authentication, especially in the industrial and business security systems.

Creating & Managing Secure Passwords

❖ One-Time Password (OTP) ...

- is commonly referred to as **OTP** in the field of software security.
- This is extensively used by the banks and other financial institutes.
- Normally **passwords** can be classified into two categories:
 - Static passwords
 - Dynamic passwords
- The static passwords are the codes saved on the server and used repeatedly for accessing the desired resources or get the physical access.
- On the other hand, the dynamic passwords are created used and discarded. They are not saved as the valid information for re-login. It is used just for one time to access the resources.
- The example of dynamic passwords is the one-time pin (OTP) used in the modern financial systems for online transactions.
- One-time pin is created when you need to accomplish some online transactions on your bank account or any other online resources.



Creating & Managing Secure Passwords

❖ One-Time Password (OTP) ...

- You login to your bank account, but every transaction regarding the movement of the funds is associated with the one-time pin or password.
- So, the **OTP** is a **type of dynamic password**, which is valid for only one transaction or session of the login.
- OTPs offer numerous advantages, which help you improve the security of critical online transactions.
- One of the most important benefits of using the OTP is that it cannot be reused for cyberattacks or any other malicious.
- So, tracking the OTP numbers will not be harmful for your account security.
- Even all past OTP generated by you are exposed to the cyber hackers; it will not make any difference at all.
- The OPTs are very difficult to be intercepted during the creation and use of those passwords.
- Thus, the use of OPTs reduces the amount of attack surface.



Creating & Managing Secure Passwords

❖ Using Password Managers ...

- In the present internet environment, we use hundreds of websites, web services, applications, and resources through internet.
- The access to the resources is validated through passwords. So, you have to remember hundreds of passwords for accessing those websites smoothly.
- If you use the same password on all websites, that means your data and personal information is in great danger for sure.
- The **identity theft** is one of the major components of the hacking attacks carried out by the cyber criminals on the internet.
- Millions of accounts and passwords are being compromised annually.



Creating & Managing Secure Passwords

❖ Using Password Managers ...

- **Two main issues** with a user regarding his/her password include the creation of strong password, and then managing the password to access the resources smoothly.
- Normally, a huge majority of the users **(1)create weak passwords** and follow the non-recommended ways for creating their passwords, which puts them at risk of cyber-attack.
- Another **(2)major problem** that the users face is to remember and manage a large number of passwords that they use for getting registered with different services and applications.
- A **good password manager** is able to solve both of those issues of a normal user.
- A **password manager** is a software application that offers the services to create a strong password and manage all those passwords in encrypted format so that they are not prone to compromise.
- A good password manager allows the user to save the encrypted password either in the cloud or on the local drives.



Creating & Managing Secure Passwords

❖ Using Password Managers ...

- Online storage of passwords in the cloud is easy to access it from anywhere in the world, but the passwords saved locally are a bit difficult to access from other locations.
- You can create multiple passwords for multiple websites and applications on the password manager that you use, but you have to **remember just one password**, which is known as the **master password**.
- You can also save and carry the saved passwords in the flash drive with you.
- There are numerous password manager like features in the major browsers like Chrome, Firefox, Internet Explorer and others, but majority of them save the passwords in plain text format not in the encrypted format, which is dangerous for you and your data.
- These passwords are not useable on the cross platforms like passwords saved on the Windows are not supported on the Linux.
- So, using a good password manager is the best and most suitable solution for an online user in today's environment of the internet.



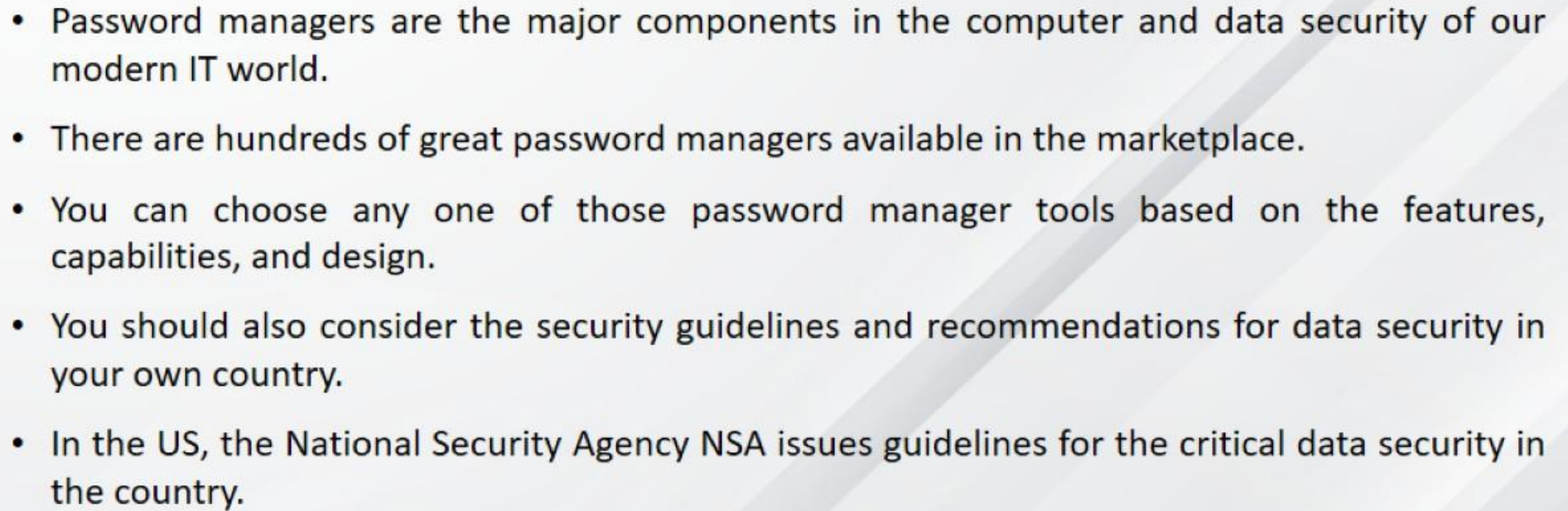
Creating & Managing Secure Passwords

❖ Using Password Managers ...

• Main Reasons to Use a Password Manager

- Generating strong passwords
 - No need to remember multiple passwords
 - No need to worry about password theft
 - Passwords stored in fully encrypted formats
 - Options to save passwords locally and in the cloud
 - Easy to access passwords
- You can create and save your passwords on password manager software tools.
 - They save your passwords in an encrypted format and they retrieve in the normal state when requested.
 - The hackers will not be able to decrypt your passwords saved on the password managers.
 - You can easily access your passwords saved in the cloud.





- Dashlane , LastPass , ZOHO Vault , KeePass , RoboForm

Password Manager Tools

❖ Dashlane ...



- Dashlane is one of the popular and password manager tools on the internet. It is available in FREE as well as paid version. It is very easy to use.
- The free version supports up to 50 passwords to create, store, and use. You can create and store your passwords with strong encryption protocols and access from anywhere around the world.
- It supports multiple browsers such as, Firefox, Chrome, Internet Explorer, and others. It also supports the mobile wallets and payment gateway password protection. More than 10,000 enterprise customers using this tool for their password security.

Password Manager Tools

❖ Dashlane ...

The other main features of Dashlane password manager include:

- It is very smooth, clean and clutter free software tool
- Supports auto-fill and auto login capabilities
- Stores and transmits password data in secure form to access
- Generates strong passwords for any new registration of service
- Use strong AES-256 encryption protocol
- Supports multiple passwords on a same website
- Offers you access through web from anywhere
- Supports Android and iOS, PC, and Macs platforms
- Supports local as well as cloud storage
- Supports one-click function to change your existing password
- Supports password migration from other services



Password Manager Tools

❖ Dashlane ...

The other main features of Dashlane password manager include:

- Allows categorization of the passwords according to critical levels
- Intuitive web interface
- Supports Chrome OS, MS Edge, and Linux
- Supports two-factor authentication
- Additional features of credit monitoring and data backup
- Supports identity theft insurance and identity restoration help
- Supports instant dark web alerts
- Support password group share for business users
- You can save personal information, IDs, receipts and payments information
- Your data is unknown to even the company employees and owners
- You can choose from multiple options and plans to use the Dashlane password manager like free, monthly plans, annual plans, and business plans.



Password Manager Tools

❖ LastPass ...

LastPass

Simplify your life.

LastPass remembers all your passwords, so you don't have to

Get LastPass Free

LastPass password manager is one of the leading names in the password security field. It is trusted by more than 43,000 enterprise customers and over 16.5 personal users.

This is an easy-to-use tool that offers high level of security of data, privacy of personal information, and fully encrypted storage of the entire information.

The interface of this password manager is very intuitive to learn without referring to any procedural documents. It offers numerous features and capabilities.

Password Manager Tools

❖ LastPass ...

A few very important features of LastPass are listed below:

- Available in both free and paid versions
- Multiple plans suitable for different segments of users
- Offers secure password vaults
- Multi-platform support like Android, iOS, Mac, PC, Windows, and others
- Smooth password access on all types of devices
- Offers auto-fill and saving options
- Offers strong password generation capabilities
- Additional feature of authenticator
- Support multifactor authentication
- Allows to create secure notes
- Supports secure sharing
- Data file storage up to 1GB
- Supports emergency access function



Password Manager Tools

❖ LastPass ...

A few very important features of LastPass are listed below:

- Fully cloud based service easy to register
- TRUSTe certified for privacy
- Supports many popular web browsers
- Supports Chrome OS and Linux
- Offers a few options for master password reset
- Easy and intuitive interface to manage and access your passwords
- Password strength alerts along with the strength scores
- Offers two-factor authentication
- Supports automatic password change
- Multiple plans available in both personal and enterprise categories
- Support auto-fill feature
- Offers capability of generating strong passwords
- Support username generating features too



Password Manager Tools

❖ LastPass ...

A few very important features of LastPass are listed below:

- Supports zero-knowledge standard, which means company does not know about your information and passwords
- Auto-fill shopping form makes your shopping experience great
- Supports storing credit card information, personal information, payment wallets and Wi-Fi information
- Offers great customer support

You can get multiple options and plans of using the LastPass password manager services that are 100% fit for your requirements.

LastPass

Simplify your life.

LastPass remembers all your passwords, so you don't have to

Get LastPass Free

Password Manager Tools

➤ ZOHIO Vault ...



ZOHIO is one of the major providers of wide range of software-based cloud services that include customer resource management, sales, marketing, communication and collaboration, finance and many others. ZOHIO vault is one of those services for personal as well as for the enterprise users. It was initially started as a free service for all. At this time, ZOHIO vault is offered not only as a free service, but also in different paid plans, which are very affordable for all types of users.

ZOHIO vault offers enterprise grade password management services through its password manager known as ZOHIO vault. It offers great features and capabilities that make it one of the popular password managers in the marketplace.

Password Manager Tools

➤ ZOHO Vault ...

The main features of ZOHO Vault password manager are listed below:

- Easy to access and manage your passwords
- Powered by the strongest AES-256 encryption standard
- Supports zero-knowledge architecture
- Easy sharing within the group of users
- Supports auto-login feature for the saved websites
- Supports different roles and levels for your password
- Single logout feature for a centralized control
- Options to easily import and export the passwords
- Centralized password management for enterprises
- You can access your passwords from anywhere and anytime
- Supports mobiles and PCs equally
- Support multiple web browsers commonly used in the marketplace
- Supports multiple operating systems including Windows, Linux, Android, Mac, iOS, Chrome OS and others



Password Manager Tools

➤ ZOHO Vault ...

The main features of ZOHO Vault password manager are listed below:

- Available in multiple plans that fit for all types of users
- A life time free plan is available
- Easy to setup and use tool
- Supports two-factor authentication
- It is lightweight service through both cloud and browser-based plugin
- Offers the features to save your personal information, social security, passport, credit card and other information
- Support auto form filling capability
- Offers the features of creating different chambers to categorize different level of security of your information and passwords
- Supports sharing of password to external users through a link and secret key
- Support the transmission of data in SSL connection

The integration of ZOHO vault with many other services offered makes it a better choice for the users of the ZOHO services. The low pricing plans are very attractive for normal users.

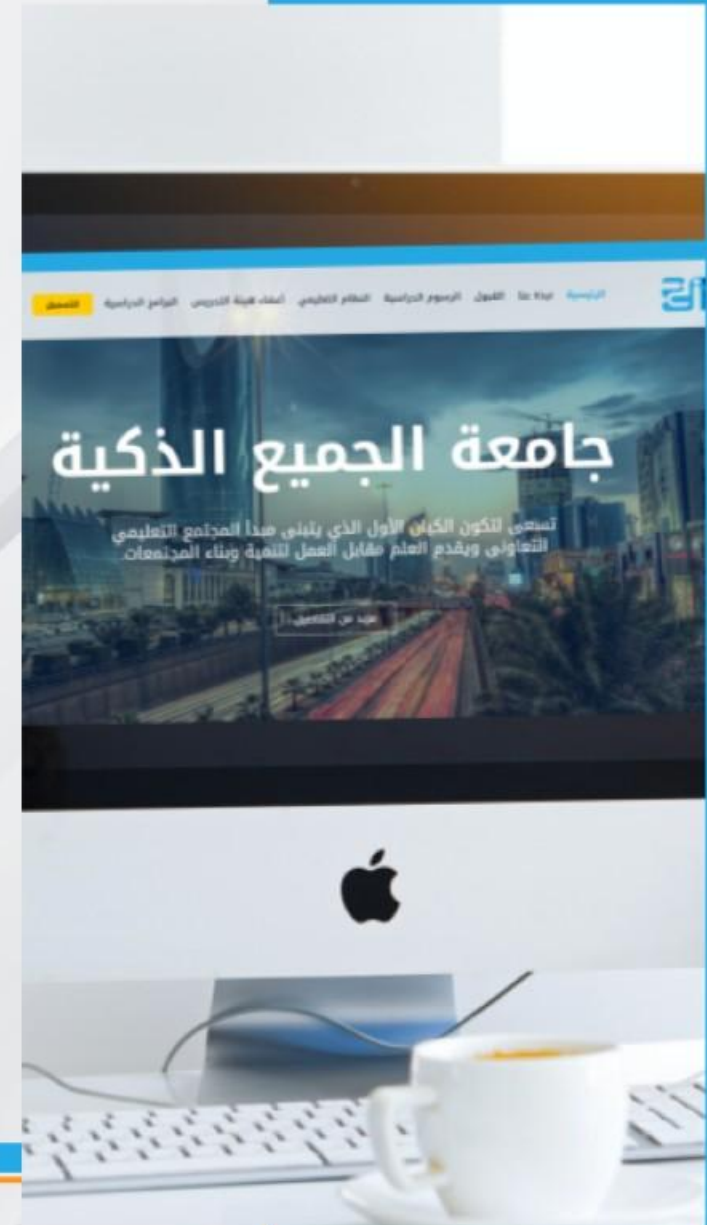


Self-Assignment

Password Manager Tools

- KeyPass
- RoboForm

The End 😊





Thank You