



Project #1 - Security

**By: Makayla. N, Ena G-C, India. C, Desja. B,
Michael. E, Emmanuel. C, Joshua. L**

Password Management System

Purpose: Password Management System: A software application or a hardware device used to store and manage a person's passwords. Password Management systems assist in generating and receiving complex passwords, potentially storing such passwords in an encrypted database or calculating them.





Max Potential Needs:

- To keep passwords safe.
- Help prevent impostor websites from stealing information.
- To ensure that employees have strong passwords.
- password managers allow employees to login via desktop computers, tablets, and phones, all while providing top-level security across devices.





GOOD PASSWORDS	BAD PASSWORDS
Be at least 8 characters in length	Spell a word or series of words that can be found in a standard dictionary
Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)	Spell a word with a number added to the beginning and the end
<ul style="list-style-type: none">- Have at least one numeric character (e.g. 0-9)- Have at least one special character (e.g. ~!@#\$%^&*()_-=)	Be based on any personal information such as user id, family name, pet, birthday, etc.
Example: Ak07@%150kzyt  * * * *	Example: 123123  * * * *

Mannie
Makayla

Options:

Ena & Makayla

Name of company:	LASTPASS	DASHLANE	KEEPER
Price:	Free, premium(\$3 mos), families(\$4 mos)	Free, premium(\$4.99 mos), premium plus(9.99 mos)	business(\$2.50 mos) Enterprise(3.75 mos)
Release Date:	August 22, 2008	October 11, 2012	January 2009
Ratings:	9/10..... 4.5/5	8/10 4/5	3/5
Pros:	<ul style="list-style-type: none"> - Strong data encryption - Affordable pricing 	<ul style="list-style-type: none"> - Auto-fills login and passwords. - Generate Strong Passwords. 	<ul style="list-style-type: none"> - Use Subfolders within main folders. - Organizes files into folders.
Cons:	<ul style="list-style-type: none"> • Limited password sharing without a subscription. 	<ul style="list-style-type: none"> • Only Work with Dashlane Browser in Android 	<ul style="list-style-type: none"> • Password autofill does not appear in the correct places.

The Efficiency Of LastPass:

Ena & makayla

- It offers a Free Version.
- Works with: Windows, MacOS, Linux, Android, iPhone and iPad. Browser extensions for Chrome, Firefox, Safari, Internet Explorer, Edge and Opera.
- Two-factor authentication.
- Password inheritance.

Overview: LastPass offers advanced password management features that few free competitors offer, and it has an updated user interface.



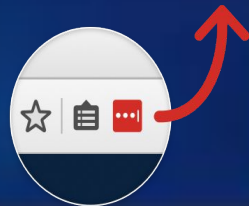
How to access/download Lastpass:

Ena

Lastpass needs to be downloaded into the employee's electronic device by the employee themselves.



- Go to: <https://www.lastpass.com/>
- On the top right corner click on the red icon that reads “Get LastPass Free”
- Create an account and fill out your personal information.
- Once the information is input and it meets all the requirements click the sign-in button.
- The sign “Welcome to LastPass!” should appear. Click the install red button that reads “Install LastPass”
- It will take you to the Chrome app store, once there click on “add to Chrome”
- Click on “Add extension”, then a file will download.
- On the top right corner, the LastPass extension should appear.
- Click on the LastPass browser button to log in.



step-by-step guide for beginners on LastPass:

- For the first time users:
→ Click on the “Show me around” button that should be located on your homepage under the “Welcome to your Vault” sign.

Welcome to your vault!

Your vault is a safe place to store passwords, notes, profiles for online shopping, and even documents. And no matter where you work, your vault keeps everything in sync, so you can stay organized and save time.

Show me around

Later

Never

step-by-step guide on how to use LastPass:

- How to add a password:

→ On your homepage click on the “+” sign.

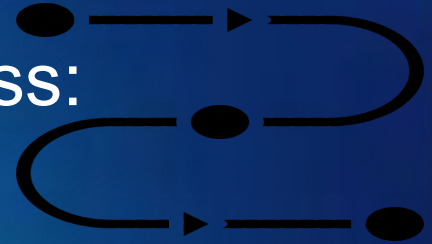


→ Then click on the password icon.



→ Fill out the information and hit save once done.

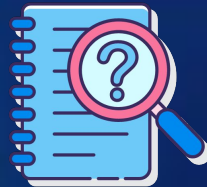
step-by-step guide on how to use LastPass:



- Tips and handling different types of information.
- Under the “Password” section. All your passwords will be located there. All in one place and safe.
- I would recommend using the “Notes” section to store important memos.
- Lastpass can also be used to keep important addresses, it might come in handy if you needed to keep an address safe.
- Payment information, as well as a digital wallet, can all be stored in LastPass as well.
- The bank account feature can be crucial if for keeping your bank account safe to secure your vault.



How do password managers work:



- Think of password managers like a digital notebook, they remember your passwords.
- All password managers perform the basics of remembering your passwords
- when you visit a site that requires you to log in, your password manager will pre-populate the usernames and passwords fields
- They also assist you with creating passwords, pointing out when the one you have chosen is too weak, or even generating them for you
- They can even alert you when a site you use has been breached. Which can lead to your information being stolen.

Overview: They take notes, store files, automatically fill forms, browse the web, generate random passwords, and diagnose your digital security.

Major goals:

Major goals: sensitize and inform employees, provide a contact person, Set and enforce policies for secure passwords, Set and enforce policies for changing passwords, and Increase productivity.



India.



Schedule:

- Step 1: Raise Awareness/Set Expectations
- Step 2: Equip
- Step 3: Implement/ Training



Step 1:

Raise Awareness/Set expectations: the knowledge and attitude of members of a company regarding the protection of the physical, and especially informational, assets of that organization

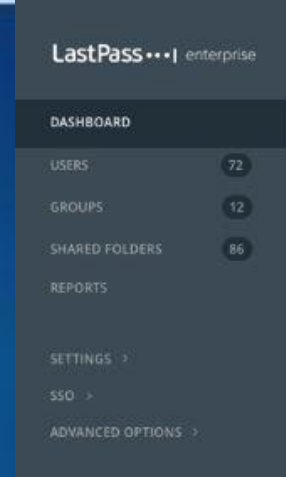
Why is it important? Security Awareness is important because it helps to prevent breaches and attacks, gains more customers, and it influences company culture

Company culture is someone's view points on security.

Makayla

Step 2:

Equip: Set up admin controls



Your CEO makes a LastPass account . Everyone that works for the company signs up and your CEO will group you accordingly to what passwords you can see. You are allowed to see the folders and reports that only your group and CEO has shared.

The CEO can see what percentage of your passwords are Secure. Also how many are Secure and the ones who aren't so before the company gets hacked the CEO can make changes.

Step 3:

Implement/Training:

- log onto: <https://www.lastpass.com/>
- On the to right corner click on the red icon that reads “Get LastPass Free”
- Create an account and fill out your personal information.
- Once the information is input and it meets all the requirements click the sign-in button.
- The sign “Welcome to LastPass!” should appear. Click install red button that reads “Install LastPass”
- It will take you to the Chrome app store, once there click on “add to Chrome”
- Click on “Add extension”, then a file will download.
- On the top right corner, the LastPass extension should appear.
- Click on the LastPass browser button to log in.

Security Awareness 1



Security Awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

Making sure that the people in the company take security serious .

- Showing proper security demonstration
- Showing new hirees that security awareness is an important thing for all tech companies
- Provide a safe network security system for all employees





What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.



Josh





Types of Viruses

- Boot Sector Virus.
- Direct Action Virus.
- Resident Virus.
- Multipartite Virus.
- Polymorphic Virus.
- Overwrite Virus.
- Spacefiller Virus.



Josh



Network Snooping, MITM, SQL Injection

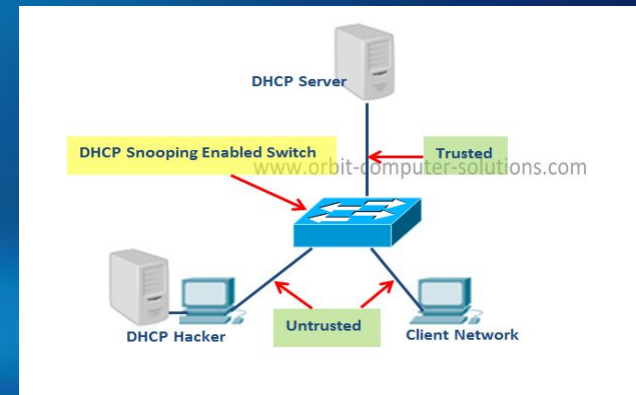
Network Snooping is unauthorized access to another person's data. For example, monitoring keystrokes, passwords, emails, etc.

Man In The Middle Attack (MITM) is an attack where a user can interfere with data communications between two parties

SQL Injections are lines of code to attack data. This allows attackers to spoof identity, tamper existing data, and much more harm



Josh

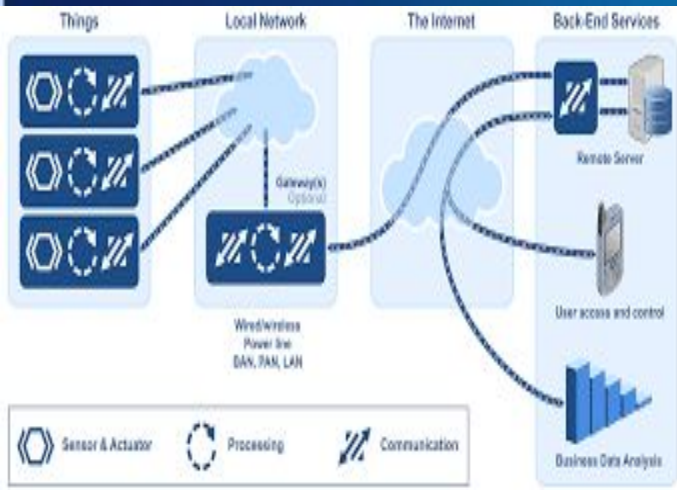


What are IoT devices?

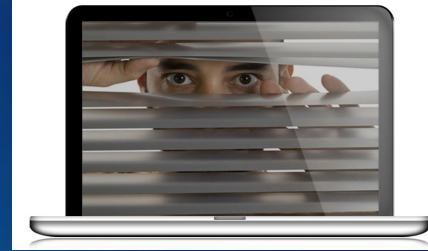
Purpose: IoT devices is a piece of hardware with a sensor that transmits data from one place to another over the internet.

Types: IoT devices can include wireless sensors, software, actuators and computer devices
Ex. USB, Micro SD, and headphones.

: IoT devices can contain malware, and if these devices are plugged into computers or other tech, they can allow the malware access to things like keystrokes, data and etc. Having knowledge about these devices can help you to watch out for them



Network Snooping



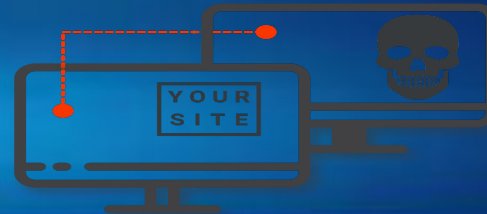
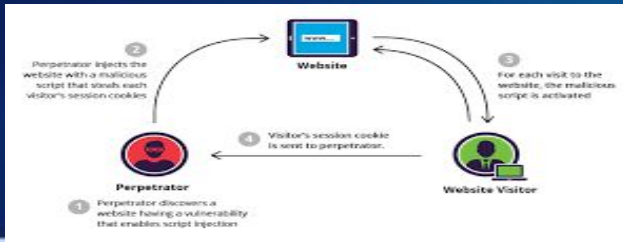
Network Snooping is unauthorized access to another person's or company's data. It's kind of like eavesdropping but it's not limited to gaining access to data during transmission. Professional snooping uses software programs to monitor activity on a computer or network device. Since networks started using more free tools for monitoring, they've become more vulnerable to attackers.

Stopping the Snoop: It starts with information and identity governance policies. Who has access to what, and when? Digital snooping is inevitable. Most users do so out of curiosity, not malicious intent, but intentions and consequences aren't always linked. Even well-meaning security employees or C-suite members could prompt a data breach or system compromise..

Cross-Site Scripting

Cross-Site Scripting is when there is a script behind a blog, email, message etc.. that will give you a virus or either hack and get all information.

Example: You was sent a vlog by a “friend” (somebody hacked them and sends to you) and you click on it and all your information gets leaked. You just thought it was a blog but what you didn’t know there was a script and now you’re hacked.



Josh & Makayla

Man in the Middle attack

Ena & Makayla

- What is it?: Man in the middle or (MITM) attacks, is when the attacker secretly positions himself in the middle of the conversation between a user and an application. The attacker can either eavesdrop or impersonate one of the parties.
- What is their goal?: the main goal of this attack to steal personal information, such as login credentials, account details and credit card numbers.
- What gets done?: during an attack, the information stolen could be used for many purposes, including identity theft, unapproved fund transfers.
- Who is mostly likely to get attack?: users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.



How to Lower your Risks of Getting Hacked

- Webroot or any other virus protection programs
- Keep your computer up to date
- Don't reuse the same password over and over
- 'Administrator' should be your default setting
- Encrypt to keep everything unreadable
- Do not open sus websites
- Do not open unrecognizable emails





Sources

- <https://www.dashlane.com/business>
- <https://www.keepersecurity.com/>
- <https://phoenixnap.com/blog/enterprise-password-management-solutions>
- <https://www.lastpass.com/password-manager>
- <https://www.makeuseof.com/tag/password-manager-features-you-need-to-know-about/>
- <https://www.cmu.edu/iso/governance/guidelines/password-management.html>
- <https://zapier.com/blog/best-password-manager/>
- <https://www.password-depot.de/en/know-how/password-management-in-companies.htm>
- <https://www.avatier.com/blog/how-to-deliver-password-management-training-to-your-employees-this-week/>