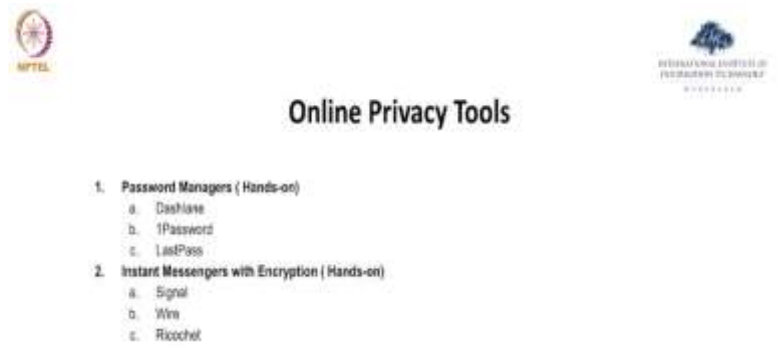
Online Privacy
International Institute of Information Technology, Hyderabad
Week 09
Part II
Online Privacy Tools

Hello, everyone, welcome to NPTEL Week-9. Part- II, in this week, we will look at another Online Privacy Tools, which are password managers and instant messengers with encryption.

(Refer Slide Time: 00:26)



Online Privacy Tools

1. Password Managers (Hands-on)
   a. Dashlane
   b. 1Password
   c. LastPass
2. Instant Messengers with Encryption (Hands-on)
   a. Signal
   b. Wire
   c. Ricochet

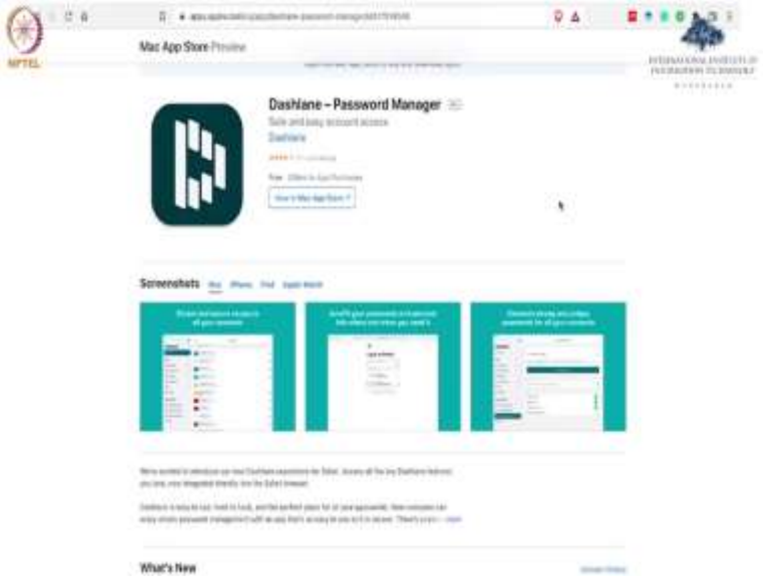
Now, first of all, let us look at what do you mean by a password manager. Password manager is a online privacy tool that helps you manage your passwords. But the question is, why do we need to manage our passwords? Why do we actually need them? So, think of a scenario, almost in our daily life, majority of people, they use very weak passwords and reuse them for different web sites. So, let us say you start your day with logging into your email, then work email, maybe social media, shopping, banking accounts, and lot more, you may enter dozens of logins and provide even personal data, your address, credit card numbers, and so on.

So, the more number of logins you have, the higher your security risk would be. And you need for password management the best practices, so the best practices to manage your password is to use Password Manager. Now, even though it is not surprising to hear somebody can ask, are password managers even safe to use? Yes, vast majority of cybersecurity specialists, they agree that the password managers are indeed the most secure way to protect your passwords.

Despite the liability of these password managers, industry as a whole, it always takes a hit after what media covers latest vulnerability, security breaches and all. But without idolizing, actually password managers, we will look at most of the important questions in the session, that how do these password managers they manage secure their passwords, what kind of technologies they are using, and what kind of architecture that they use and different servers.

So, such kind of scenarios, we will look in this hands-on session. So, there are permanently 3 kind of password managers, Dashlane, 1password and LastPass. So, I will first walk you through the Dashlane architecture, How it is being.

(Refer Slide Time: 02:54)



Mac App Store Preview

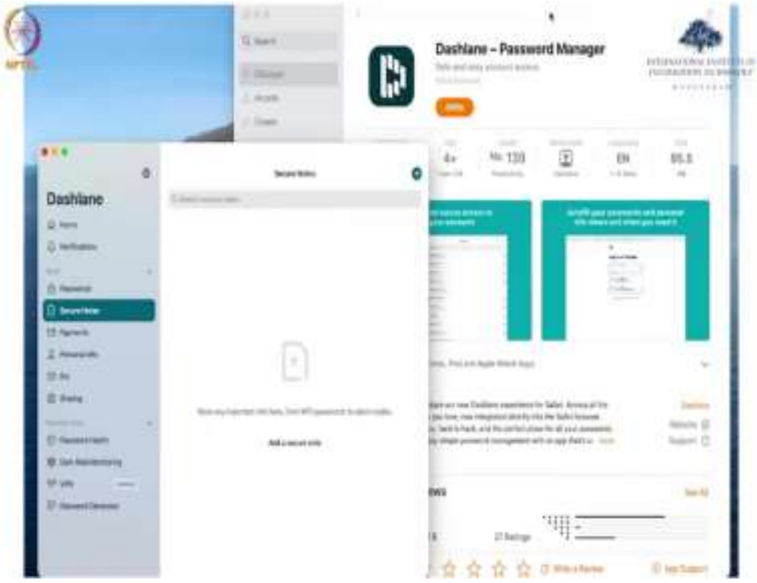
Dashlane – Password Manager

Screenshots

What's New

So, Dashlane Password Manager, so this password manager is a little bit newer, but they lack name recognition and all, although they are present for almost all the apps, Windows, OS apps, iPhone, iPad, Android and they also have extensions for every browser features, security, dashboard that analyzes your password, and they can even have an automatic password changer that can help you to change your passwords so that, you do not have to deal with yourself. So, on my screen, you can see the Dashlane Password Manager, if you want to get it for the MacBook, then you can view it in the app store.

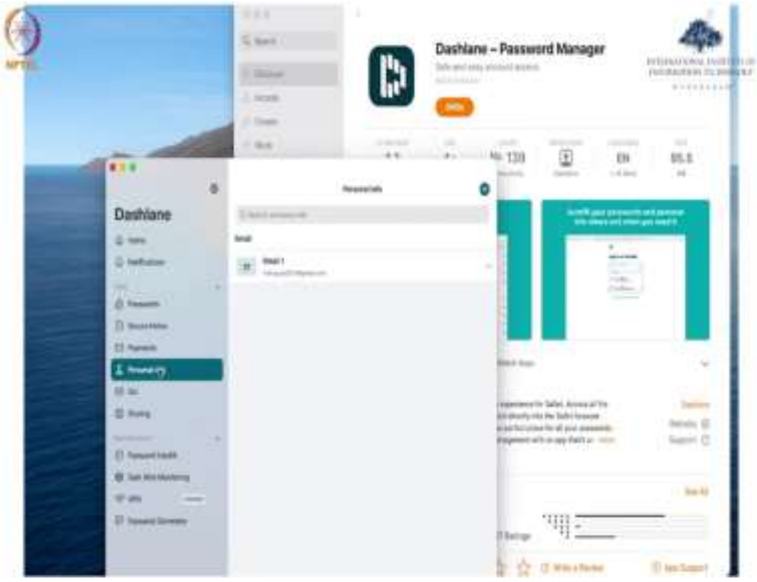
(Refer Slide Time: 03:38)

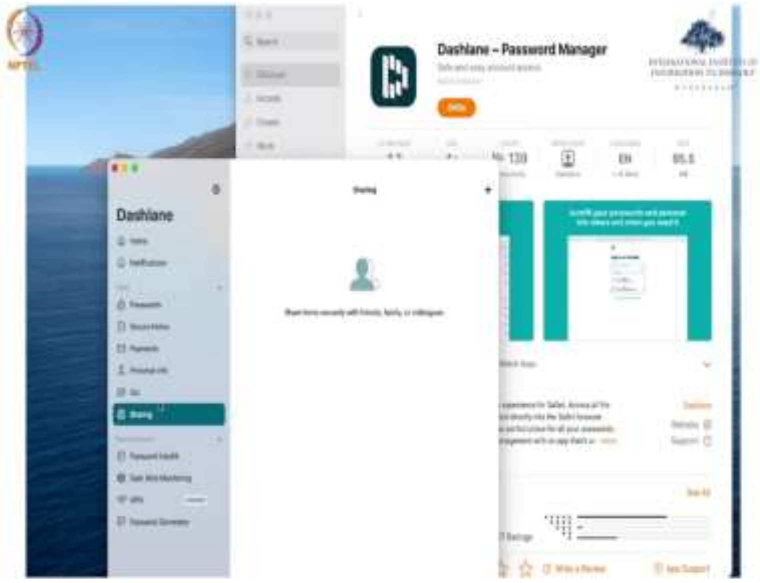


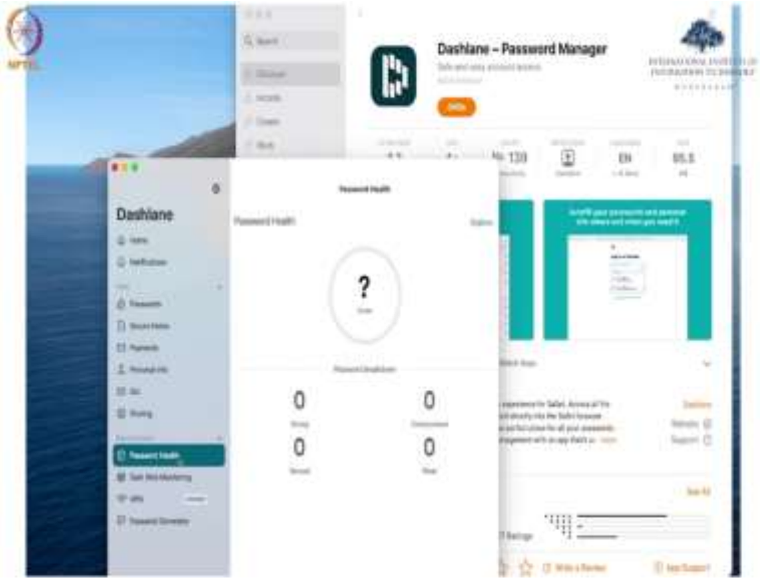
I have already get it from the App Store. So, you can see on my screen the icon is open. So, it is quite new. Now you can see here that on the left-hand side, one of the best feature of this particular Dashlane Password Manager is that it is completely free to use on a single device. So, if you have to sync your passwords between devices, then you have to update for the premium service.

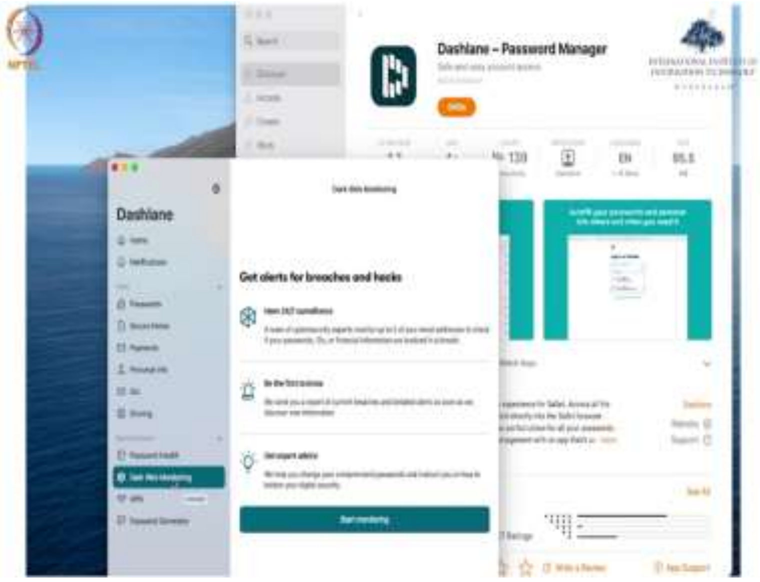
Now, when it comes to security, Dashlane, it has another advantage because you have the choice to keep your old passwords locally on your computer rather than in cloud. That is a great feature, great advantage.

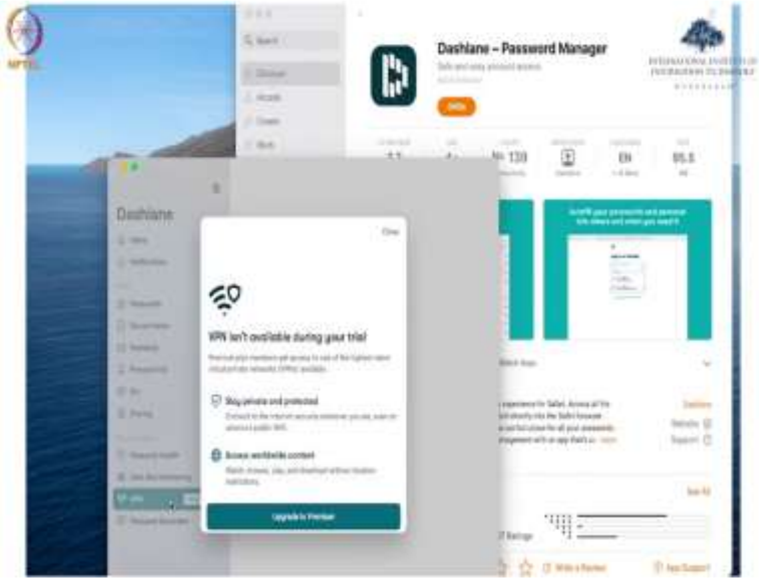
(Refer Slide Time: 04:32)




Dashlane – Password Manager
No. 139
EN
95.5
Dashlane
Home
Notifications
Passwords
Secure Notes
Payments
Personal Info
IDs
Sharing
Password Health
Dark Web Monitoring
VPN
Password Generator
Sharing
+


Dashlane – Password Manager
No. 139
EN
95.5
Dashlane
Home
Notifications
Passwords
Secure Notes
Payments
Personal Info
IDs
Sharing
Password Health
Dark Web Monitoring
VPN
Password Generator
Password Health
Password Health
?
0
0
0
0


Dashlane – Password Manager
No. 139
EN
95.5
Dashlane
Home
Notifications
Passwords
Secure Notes
Payments
Personal Info
IDs
Sharing
Password Health
Dark Web Monitoring
VPN
Password Generator
Dark Web Monitoring
Get alerts for breaches and hacks
Start monitoring



Dashlane – Password Manager

Dashlane

VPN isn't available during your trial

Stay private and protected

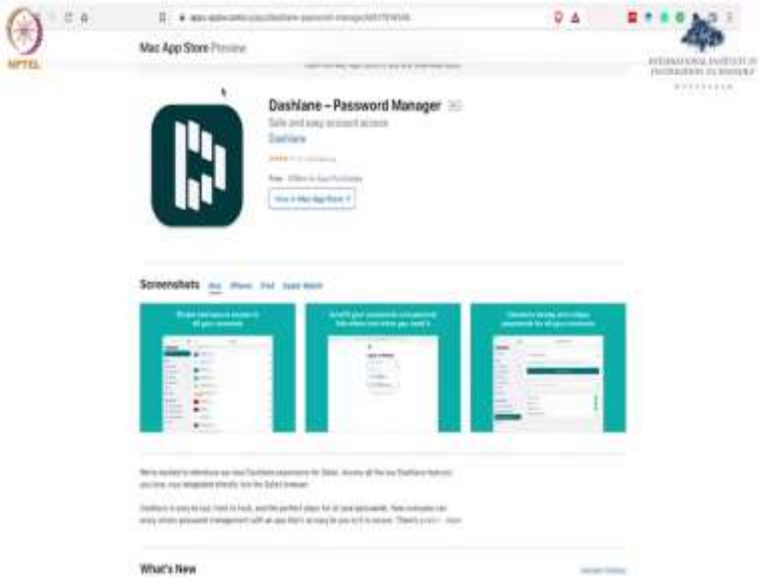
Access worldwide content

Upgrade to Premium

Now you can see here that you can store your personal information, sharing, password health, you can check using the Dashlane, you can manage your password health, then there is also a feature called Dark Web monitoring. This feature helps you to look for scan for compromised information and make changes quickly.

Then you can also secure your Wi Fi connection using with a virtual private network VPN that we have already studied in the previous lecture, it also provides 2-factor authentication which is 2FA.

(Refer Slide Time: 05:17)



Mac App Store Preview

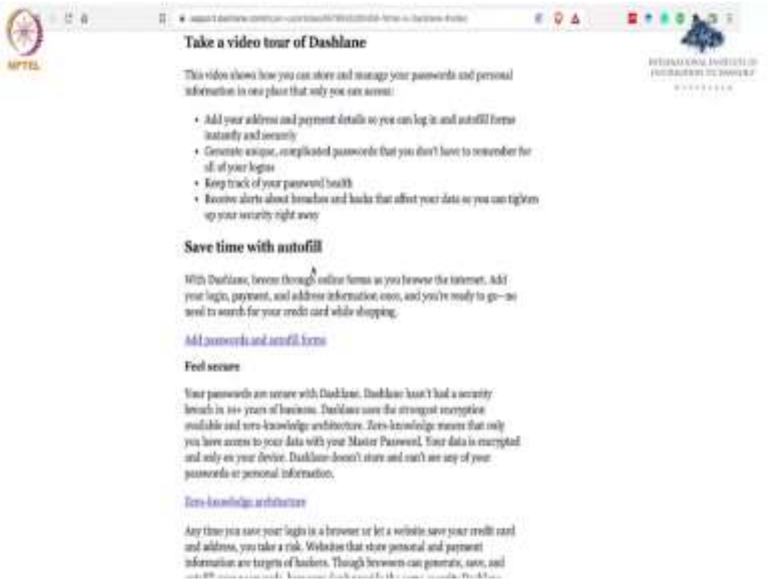
Dashlane – Password Manager

Safe and easy account access

Dashlane

Screenshots

What's New



Take a video tour of Dashlane

This video shows how you can store and manage your passwords and personal information in one place that only you can access:

- Add your address and payment details so you can log in and autofill forms instantly and securely
- Generate unique, complicated passwords that you don't have to remember for all of your logins
- Keep track of your password health
- Receive alerts about breaches and hacks that affect your data so you can tighten up your security right away

Save time with autofill

With Dashlane, breeze through online forms as you browse the internet. Add your login, payment, and address information once, and you're ready to go—no need to search for your credit card while shopping.

Add passwords and autofill forms

Feel secure

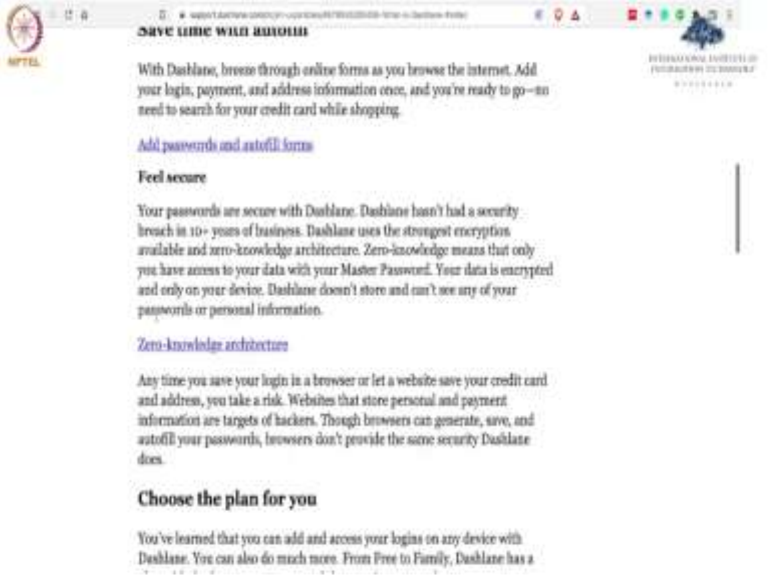
Your passwords are secure with Dashlane. Dashlane hasn't had a security breach in 10+ years of business. Dashlane uses the strongest encryption available and zero-knowledge architecture. Zero-knowledge means that only you have access to your data with your Master Password. Your data is encrypted and only on your device. Dashlane doesn't store and can't see any of your passwords or personal information.

Zero-knowledge architecture

Any time you save your login in a browser or let a website save your credit card and address, you take a risk. Websites that store personal and payment information are targets of hackers. Though browsers can generate, save, and

Now I can, I can help you go through the support that kind of, tour how can you actually take a video tour of the Dashlane. So, you need to add your address and payment details when you log in auto. So, for the free version you need not to enter any details here. But the main, major feature is that it saves you to auto, saves your time to fill the passwords using the autofill feature.

(Refer Slide Time: 05:50)



Save time with autofill

With Dashlane, breeze through online forms as you browse the internet. Add your login, payment, and address information once, and you're ready to go—no need to search for your credit card while shopping.

Add passwords and autofill forms

Feel secure

Your passwords are secure with Dashlane. Dashlane hasn't had a security breach in 10+ years of business. Dashlane uses the strongest encryption available and zero-knowledge architecture. Zero-knowledge means that only you have access to your data with your Master Password. Your data is encrypted and only on your device. Dashlane doesn't store and can't see any of your passwords or personal information.

Zero-knowledge architecture

Any time you save your login in a browser or let a website save your credit card and address, you take a risk. Websites that store personal and payment information are targets of hackers. Though browsers can generate, save, and autofill your passwords, browsers don't provide the same security Dashlane does.

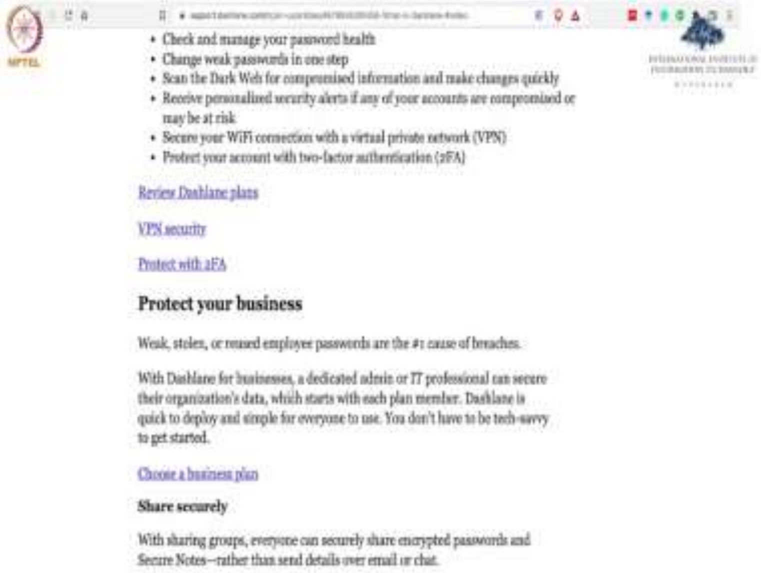
Choose the plan for you

You've learned that you can add and access your logins on any device with Dashlane. You can also do much more. From Free to Family, Dashlane has a

Then, most important architecture is the Zero knowledge architecture. So, this will not store your any of the information personal payment information on their servers. So, therefore, without saving this kind of information, personal information, you can access your data with just 1 master password. So, for the password manager, you will have only 1 master password that you need to remember.

And it uses a strong encryption, which is storing your password in the encrypted form on your device. Second, it is better than these browser logins. Because the browser's logging they do not provide same security as Dashlane provides.

(Refer Slide Time: 06:46)



- Check and manage your password health
- Change weak passwords in one step
- Scan the Dark Web for compromised information and make changes quickly
- Receive personalized security alerts if any of your accounts are compromised or may be at risk
- Secure your WiFi connection with a virtual private network (VPN)
- Protect your account with two-factor authentication (2FA)

Review Dashlane plans

VPN security

Protect with 2FA

Protect your business

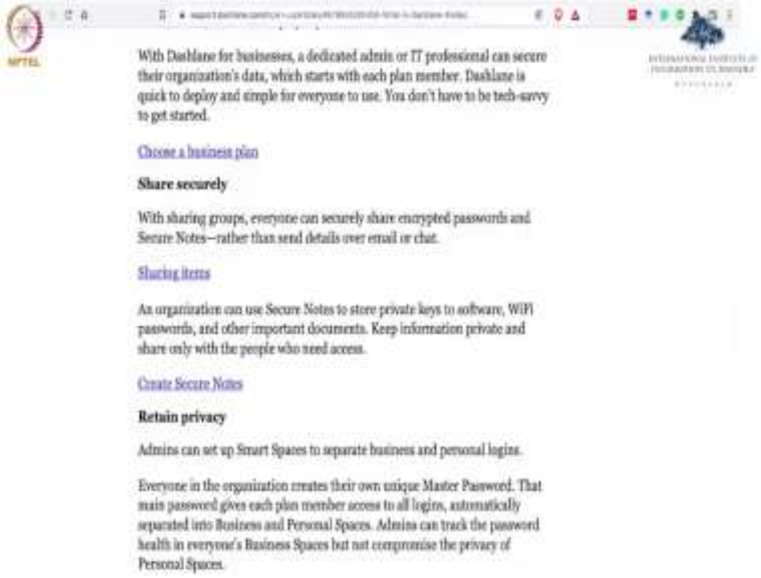
Weak, stolen, or reused employee passwords are the #1 cause of breaches.

With Dashlane for businesses, a dedicated admin or IT professional can secure their organization's data, which starts with each plan member. Dashlane is quick to deploy and simple for everyone to use. You don't have to be tech-savvy to get started.

Choose a business plan

Share securely

With sharing groups, everyone can securely share encrypted passwords and Secure Notes—rather than send details over email or chat.



With Dashlane for businesses, a dedicated admin or IT professional can secure their organization's data, which starts with each plan member. Dashlane is quick to deploy and simple for everyone to use. You don't have to be tech-savvy to get started.

Choose a business plan

Share securely

With sharing groups, everyone can securely share encrypted passwords and Secure Notes—rather than send details over email or chat.

Sharing items

An organization can use Secure Notes to store private keys to software, WiFi passwords, and other important documents. Keep information private and share only with the people who need access.

Create Secure Notes

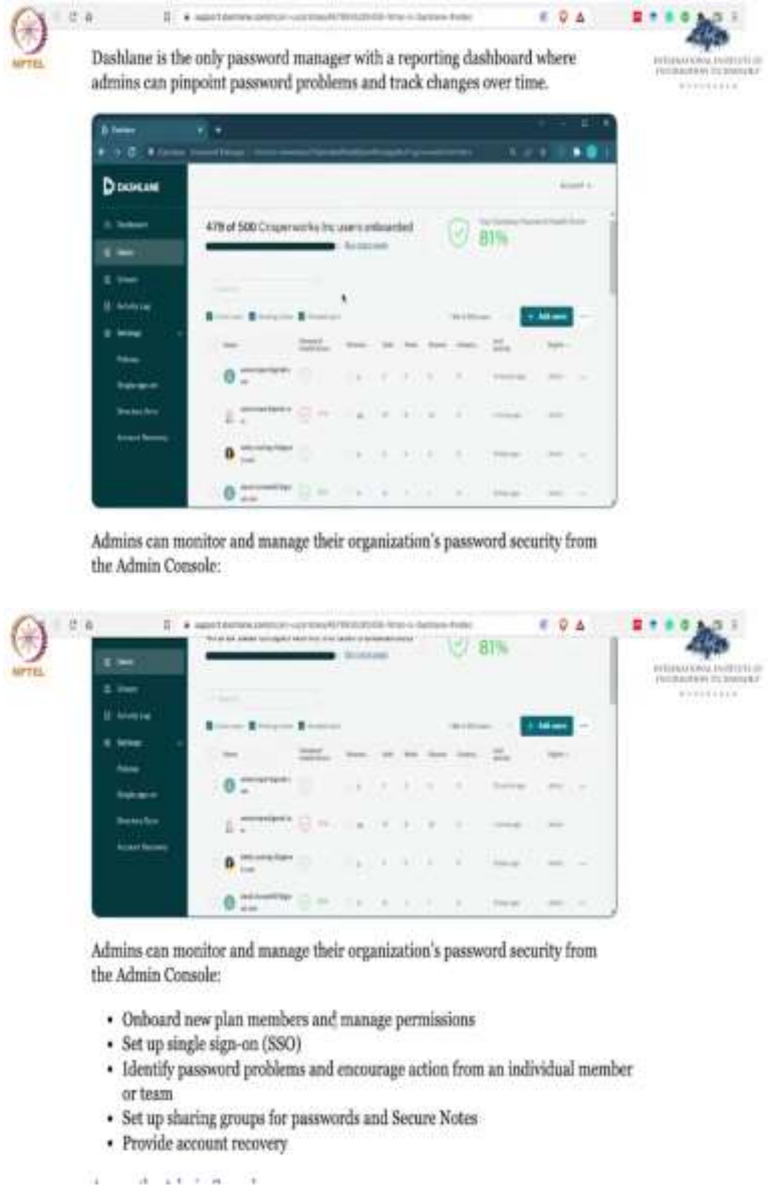
Retain privacy

Admins can set up Smart Spaces to separate business and personal logins.

Everyone in the organization creates their own unique Master Password. That main password gives each plan member access to all logins, automatically separated into Business and Personal Spaces. Admins can track the password health in everyone's Business Spaces but not compromise the privacy of Personal Spaces.

And then there are different plans that you can choose, we have already seen 2FA, 2factor authentication. And then within the groups, you can securely share your encrypted passwords rather than send details over email or chat. That is also one of the important feature. Basically admins, they can set up smart spaces to separate business and personal logins, which retain their privacy.

(Refer Slide Time: 07:15)



Dashlane is the only password manager with a reporting dashboard where admins can pinpoint password problems and track changes over time.

Admins can monitor and manage their organization's password security from the Admin Console:

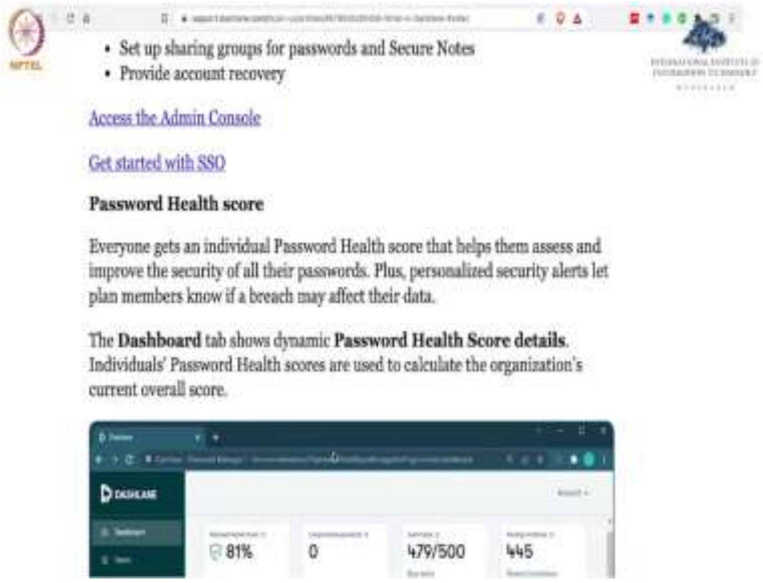
Admins can monitor and manage their organization's password security from the Admin Console:

- Onboard new plan members and manage permissions
- Set up single sign-on (SSO)
- Identify password problems and encourage action from an individual member or team
- Set up sharing groups for passwords and Secure Notes
- Provide account recovery

So, this is the only Password Manager which has this reporting dashboard where admins can pinpoint password problems track changes over time to all the users, so within an organization, it becomes very easy to store the passwords using such kind of password managers. So, you can also see here that onboard new plan members and how can we manage permissions, set up a single sign in SSO, identify password problems.

So, some of you might be working with the industry, in industry might be popping up periodically, that your password needs a change, you need to encourage action from a individual member or team, you need to set up, up sharing groups for passwords and Secure Notes and provide account recovery.

(Refer Slide Time: 08:06)



- Set up sharing groups for passwords and Secure Notes
- Provide account recovery

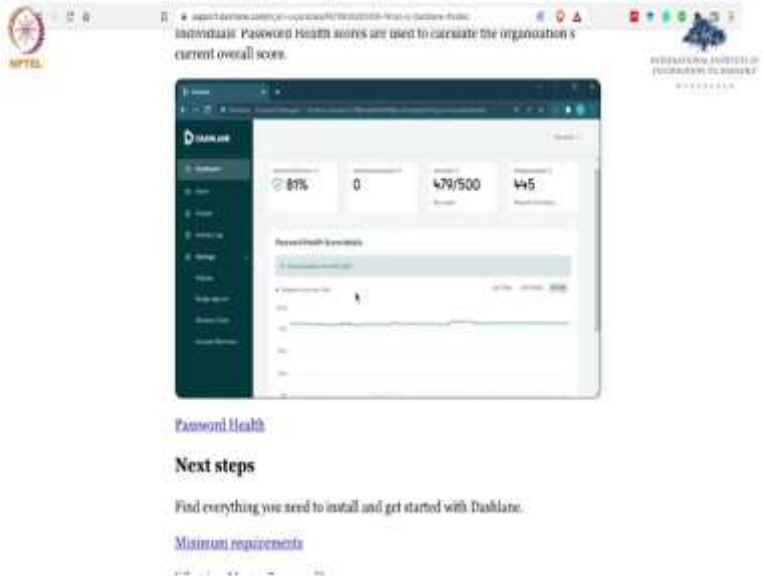
Access the Admin Console

Get started with SSO

Password Health score

Everyone gets an individual Password Health score that helps them assess and improve the security of all their passwords. Plus, personalized security alerts let plan members know if a breach may affect their data.

The **Dashboard** tab shows dynamic **Password Health Score details**. Individuals' Password Health scores are used to calculate the organization's current overall score.



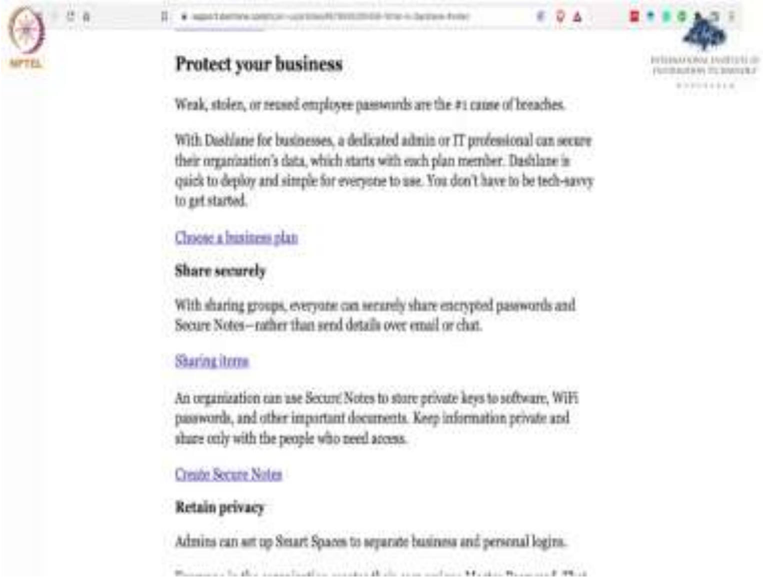
Individuals' Password Health scores are used to calculate the organization's current overall score.

Password Health

Next steps

Find everything you need to install and get started with Dashlane.

Minimum requirements



Protect your business

Weak, stolen, or reused employee passwords are the #1 cause of breaches.

With Dashlane for businesses, a dedicated admin or IT professional can secure their organization's data, which starts with each plan member. Dashlane is quick to deploy and simple for everyone to use. You don't have to be tech-savvy to get started.

Choose a business plan

Share securely

With sharing groups, everyone can securely share encrypted passwords and Secure Notes—rather than send details over email or chat.

Sharing items

An organization can use Secure Notes to store private keys to software, WiFi passwords, and other important documents. Keep information private and share only with the people who need access.

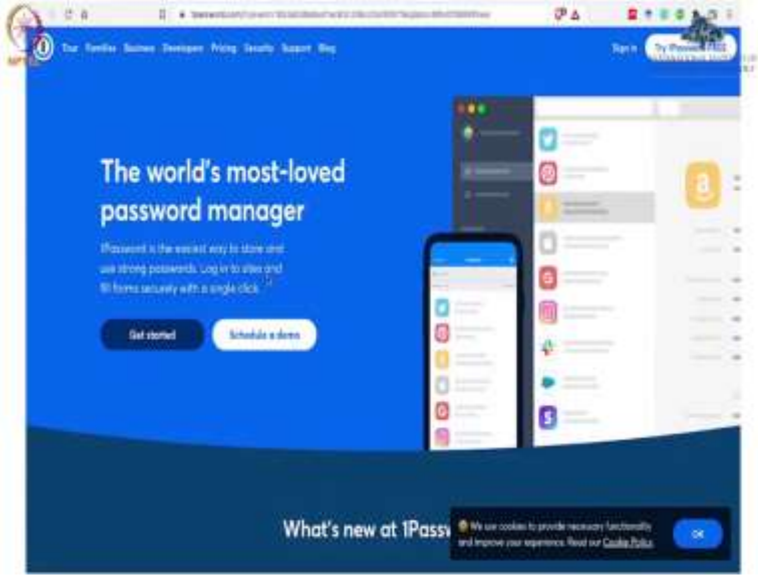
Create Secure Notes

Retain privacy

Admins can set up Smart Spaces to separate business and personal logins.

Then this password manager also returns you or checks your password health score that helps you to access and improve the security of your passwords. So, these are the details that you can see here Dashlane password health score is 81 percent. And then then this is the very nice graph that is made based on your data of last 7 days and 30 days. So, there are different options so this is the support website, support dot dashlane dot com, which you can visit for all the tutorials and further on.

(Refer Slide Time: 09:07)

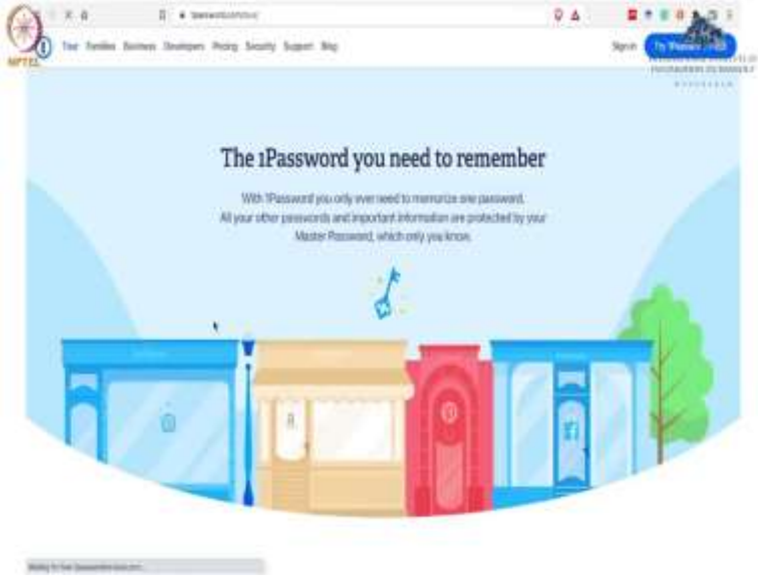

Tour Families Business Developers Pricing Security Support Blog
Sign in
Try 1Password FREE
Get started
Schedule a demo
OK

The world's most-loved password manager

1Password is the easiest way to store and use strong passwords. Log in to sites and fill forms securely with a single click.

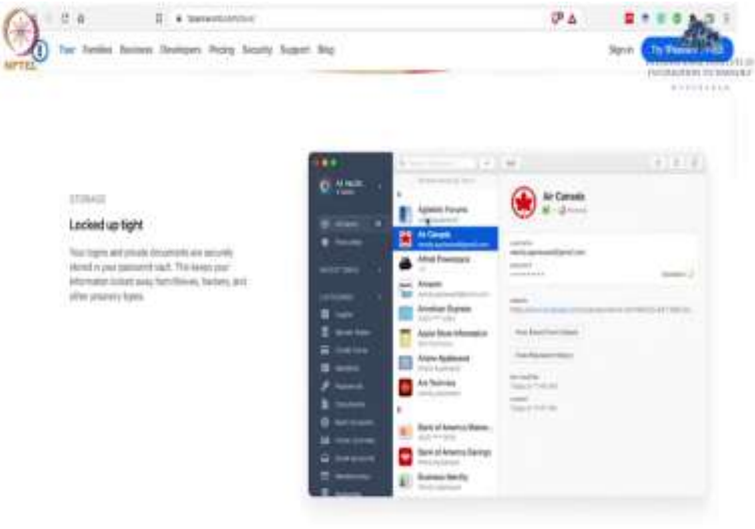
What's new at 1Passw

We use cookies to provide necessary functionality and improve your experience. Read our Cookie Policy.


Tour Families Business Developers Pricing Security Support Blog
Sign in
Try 1Password FREE

The 1Password you need to remember

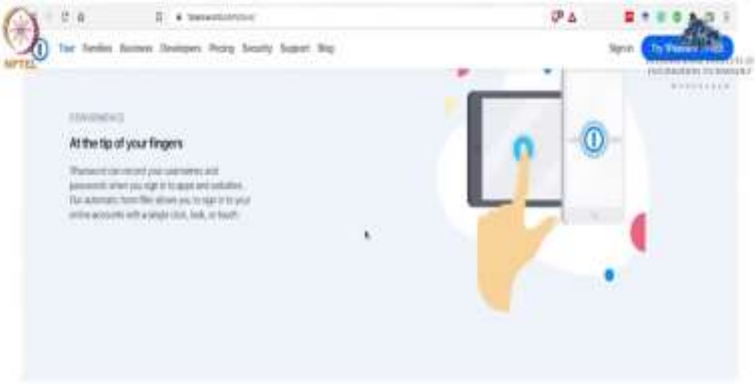
With 1Password you only ever need to memorize one password. All your other passwords and important information are protected by your Master Password, which only you know.


Tour Families Business Developers Pricing Security Support Blog
Sign in
Try 1Password free
Air Canada

STORAGE

Locked up tight

Your logins and private documents are securely stored in your password vault. This keeps your information locked away from thieves, hackers, and other unsavory types.


Tour Families Business Developers Pricing Security Support Blog
Sign in
Try 1Password free

CONVENIENCE

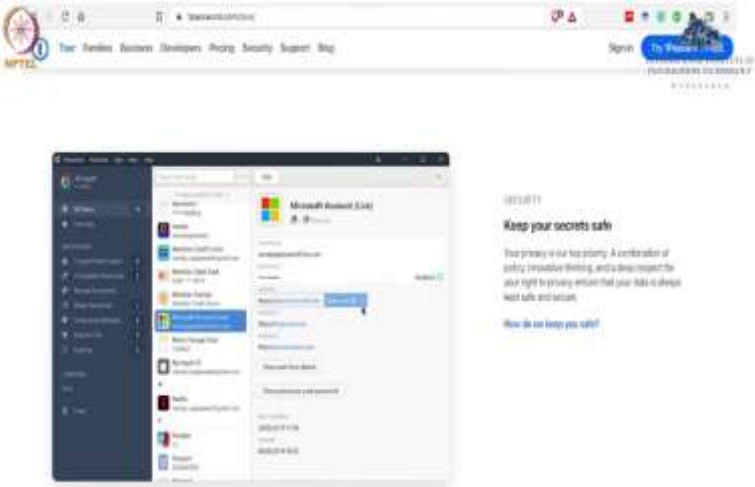
At the tip of your fingers

1Password can record your usernames and passwords when you sign in to apps and websites. Our automatic form filler allows you to sign in to your online accounts with a single click, look, or touch.

SECURITY

Keep your secrets safe

Your privacy is our top priority. A combination of policy, innovative thinking, and a deep respect for

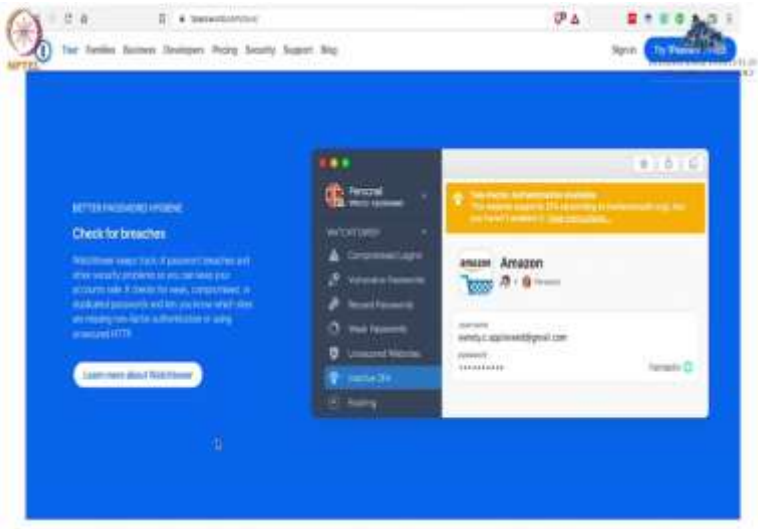

Tour Families Business Developers Pricing Security Support Blog
Sign in
Try 1Password free
Microsoft Account (Live)

SECURITY

Keep your secrets safe

Your privacy is our top priority. A combination of policy, innovative thinking, and a deep respect for your right to privacy ensures that your data is always kept safe and secure.

How do we keep you safe?



Next, let us have a look at another password manager which is 1password. So, 1password it is one of the easiest way to store and use strong passwords login into websites on just a single click. So, one of the most prominent feature it protects your data with top most security features, convenient, intuitive dashboard you can see pricing as well.

So, this is tested on Windows, Macbook Air, Android, iOS, smartphones, multiple password vaults are possible and 2 factor authentication, it is similar to that of Dashlane then autosave and autofill password feature is also present in the 1 password.

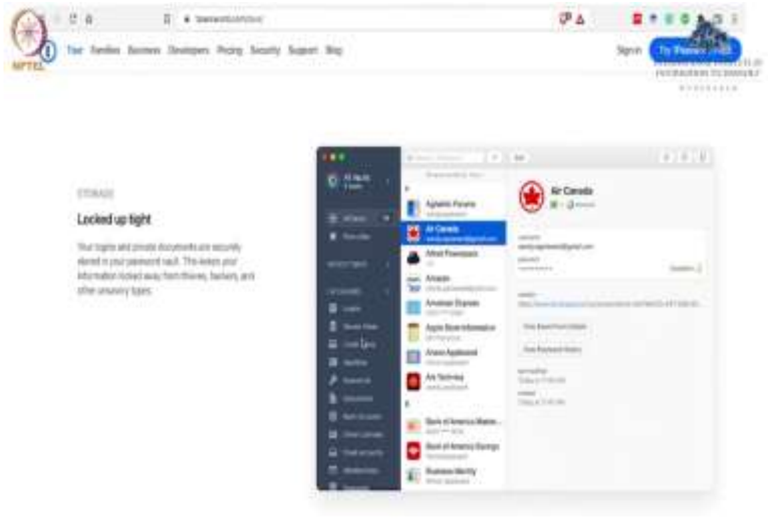
So, it is basically has a lot of features. You can see here the tool, 1 password tool that you can take locked up tight. You can see here, the window of the 1 password. So, basically on the right-hand side, you can see that you can try 1 password for free. And as it shows you in the screenshot that there are 3 vaults and depending upon what kind of, you can organize basically your personal, financial, travel, work and family passwords and data. Different kinds of vaults corresponding to that.

Then you have also password monitoring feature, which shows you alerts regarding if your passwords are weak, one label, duplicate and breached. So, one of the important feature is that you can set your travel mode. So, in the travel mode, you can actually hide your important passwords when you travel outside the country. So, it is only one of the password manager that provides you this tool travel mode.

So, this 1 password, it also has this browser extension. Then you can see here that on the one tip of your finger, you can actually set keep your passwords safe. And you have these you our browser add-ons as you see on the right-hand side. So, this will help you to sync your passwords seamlessly between the devices.

Now, there are also ways to check for the breaches and the 1 password and there are different plans that are available. And it uses 256-bit AES encryption and extremely user friendly 1 password manager. So, basically, virtual payment cards are also one of the security features that are available in this 1 password mode.

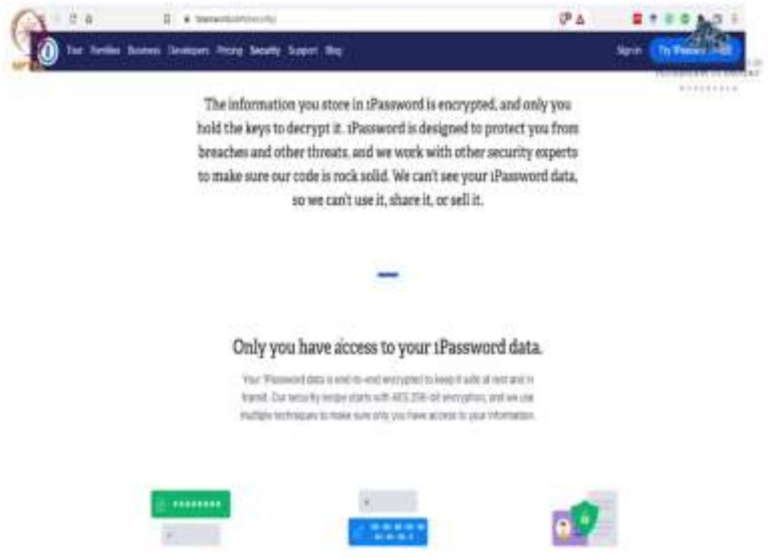
(Refer Slide Time: 11:55)



STORAGE

Locked up tight

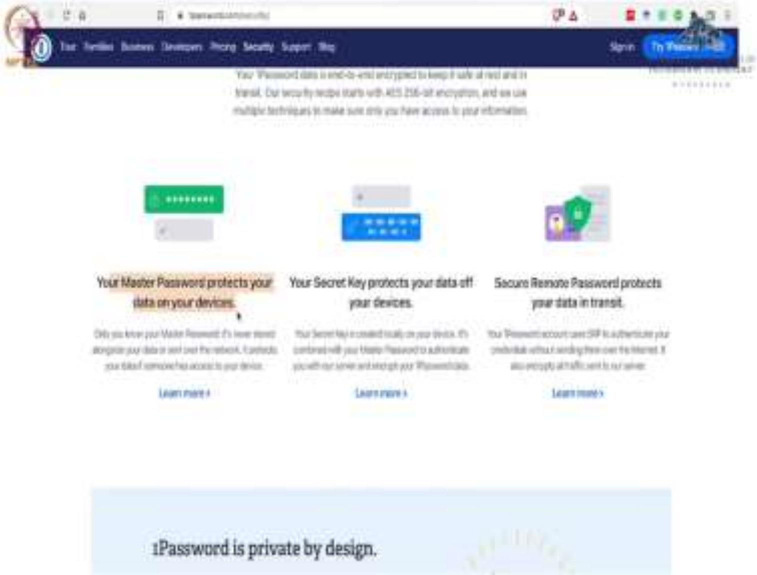
Your logins and private documents are securely stored in your password vault. This keeps your information locked away from thieves, hackers, and other unsavory types.



The information you store in 1Password is encrypted, and only you hold the keys to decrypt it. 1Password is designed to protect you from breaches and other threats, and we work with other security experts to make sure our code is rock solid. We can't see your 1Password data, so we can't use it, share it, or sell it.

Only you have access to your 1Password data.

Your 1Password data is end-to-end encrypted to keep it safe at rest and in transit. Our security recipe starts with AES 256-bit encryption, and we use multiple techniques to make sure only you have access to your information.



Your 1Password data is end-to-end encrypted to keep it safe at rest and in transit. Our security recipe starts with AES 256-bit encryption, and we use multiple techniques to make sure only you have access to your information.

Your Master Password protects your data on your devices.

Only you know your Master Password: it's never stored alongside your data or sent over the network. It protects your data if someone has access to your device.

Learn more ›

Your Secret Key protects your data off your devices.

Your Secret Key is created locally on your device. It's combined with your Master Password to authenticate you with our server and encrypt your 1Password data.

Learn more ›

Secure Remote Password protects your data in transit.

Your 1Password account uses SRP to authenticate your credentials without sending them over the internet. It also encrypts all traffic sent to our server.

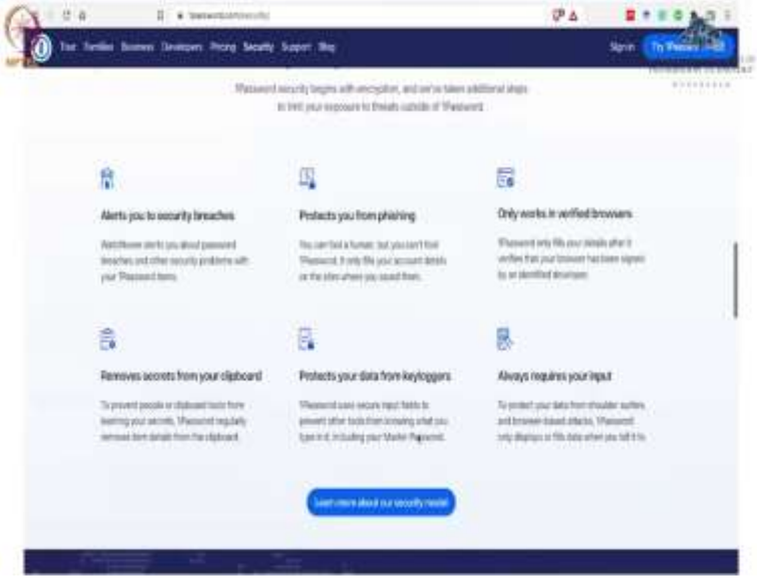
Learn more ›

1Password is private by design.

You can also do this clip, clipboard customization you can see here that this customization of vaults and secure notes, credit cards, identities password, this all you can secure. So, this is similarly you can see here that there are different kinds of security we know that only you hold the keys to decrypt this.

So, the security feature is very nice that your Master Password protect your data on all the devices. Your secret key protects your data off your devices and secure remote password protects your data in the transit. So, it is private by design.

(Refer Slide Time: 12:43)



1Password security begins with encryption, and we've taken additional steps to limit your exposure to threats outside of 1Password.

Alerts you to security breaches

Watchtower alerts you about password breaches and other security problems with your 1Password items.

Protects you from phishing

You can fool a human, but you can't fool 1Password. It only fills your account details on the sites where you saved them.

Only works in verified browsers

1Password only fills your details after it verifies that your browser has been signed by an identified developer.

Removes secrets from your clipboard

To prevent people or clipboard tools from learning your secrets, 1Password regularly removes item details from the clipboard.

Protects your data from keyloggers

1Password uses secure input fields to prevent other tools from knowing what you type in it, including your Master Password.

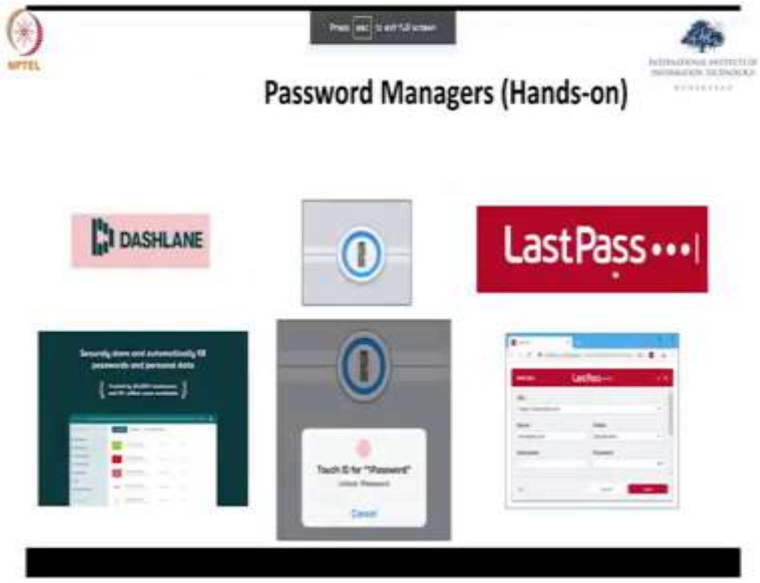
Always requires your input

To protect your data from shoulder surfers and browser-based attacks, 1Password only displays or fills data when you tell it to.

Learn more about our security model

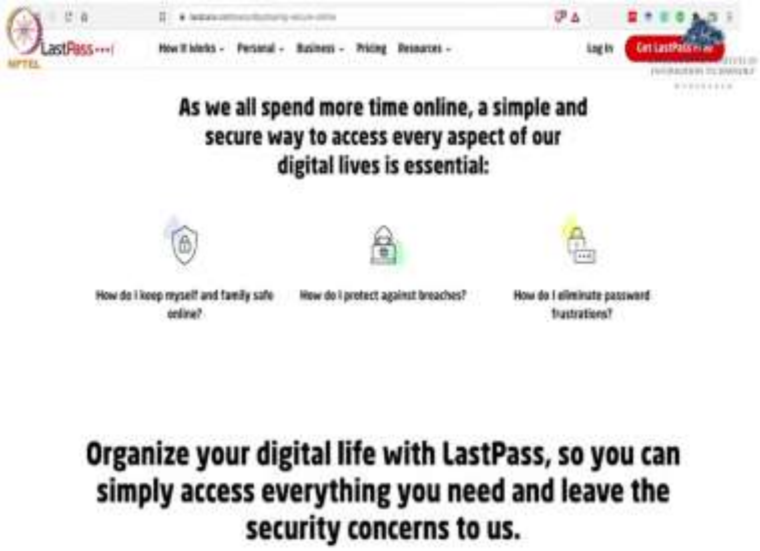
So, you can read all the security features here it protects you from phishing, key loggers, always require your input to protect your data form shoulder surfing and browser-based attacks, it displays your file fill, it displays or fills data what you tell it to do. And removes all the secrets from the clipboard. And so one of the great features of 1 password. So, next we will have a look at what is our next Password Manager which is, let me go to, yeah.

(Refer Slide Time: 13:24)


NPTEL
Press esc to exit full screen

Password Managers (Hands-on)

DASHLANE
LastPass•••|
Securely store and automatically fill passwords and personal data
Touch ID for "Password"
Cancel



As we all spend more time online, a simple and secure way to access every aspect of our digital lives is essential:

How do I keep myself and family safe online?

How do I protect against breaches?

How do I eliminate password frustrations?

Organize your digital life with LastPass, so you can simply access everything you need and leave the security concerns to us.

Effortless security for your digital life

Access everything you need online simply and securely, wherever you're logging in from.

As we all spend more time online, a simple and secure way to access every aspect of our digital lives is essential:

The next Password Manager is LastPass. So, yeah LastPass we can look at its website. So, after 1 password, we have already seen that Dashlane and 1 password, these are 2 different password manager. Now why we what is new in this LastPass, so it is basically you can see here that it is available open source LastPass. And this is a cloud-based password managers.

So, right now are the previous password managers. They were storing your passwords and all on your device, but it is a cloud based. So, some people they prefer cloud-based Password Manager extensions, mobile apps, desktop apps.

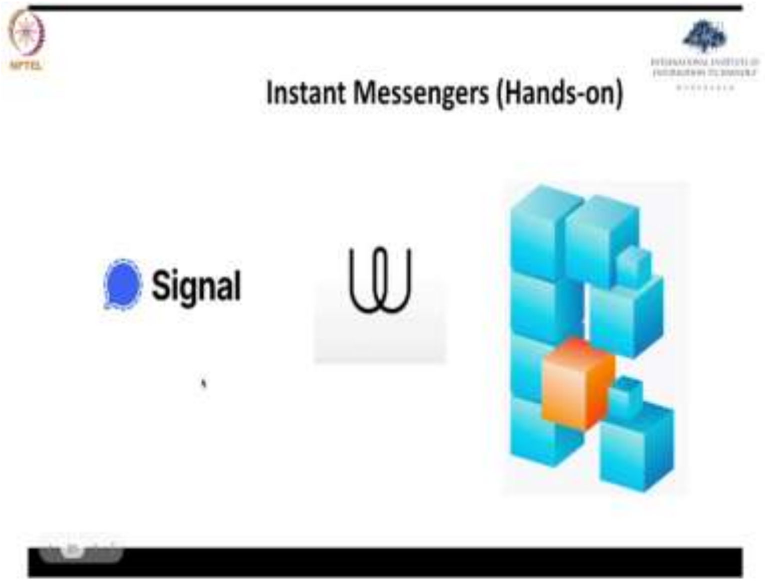
Similarly, 2 factor authentication is same. But here it is not for everyone but those who are only comfortable with cloud-based management. And it has more features in its free version that is most important thing. And more reliable. It is.

So, recently LastPass has faced a security breach that basically tells its history. But there was no data that was compromised in this breach. And LastPass encryption system is very nice. But there are some of the vulnerabilities that so actually, the question is that if somebody asked that, what happens if a password manager get compromised, how we will deal with such kind of vulnerabilities, what kind of damage can occur to the customer.

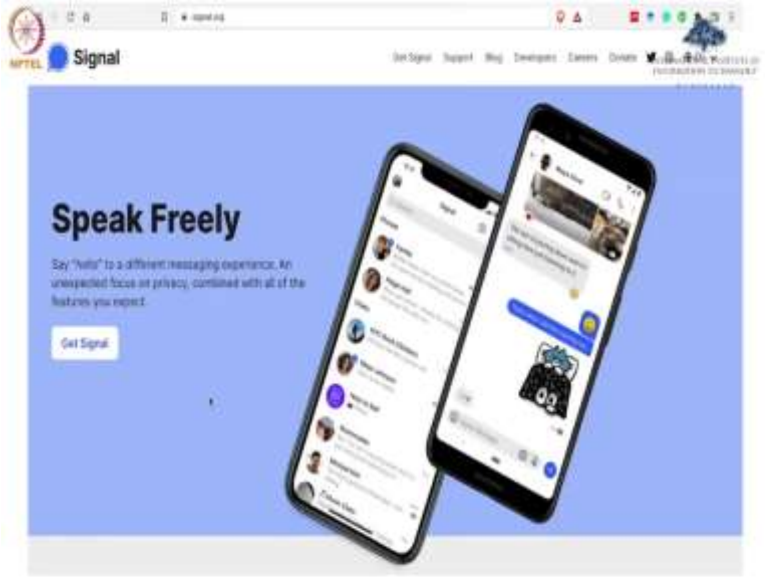
So, if we will see the history of the last pass in 2015, around LastPass, it detected some intrusion on its servers and hackers, they were trying to use the email address and password reminders. But there was more damage that was done because even if you use the any weak password, weak master password for the password manager, the attackers even crack it, they will still need to verify through your email only.

So, in 2016, also, there were some vulnerabilities that were reported in the LastPass and so on. But it can be used on the multiple devices and multi devising feature is available in LastPass premium version only. Now, so, this makes it different from the Dashlane, where it does not support multiple devices of any type. In its free version, and you can strictly get it only on 1 device.

(Refer Slide Time: 16:40)

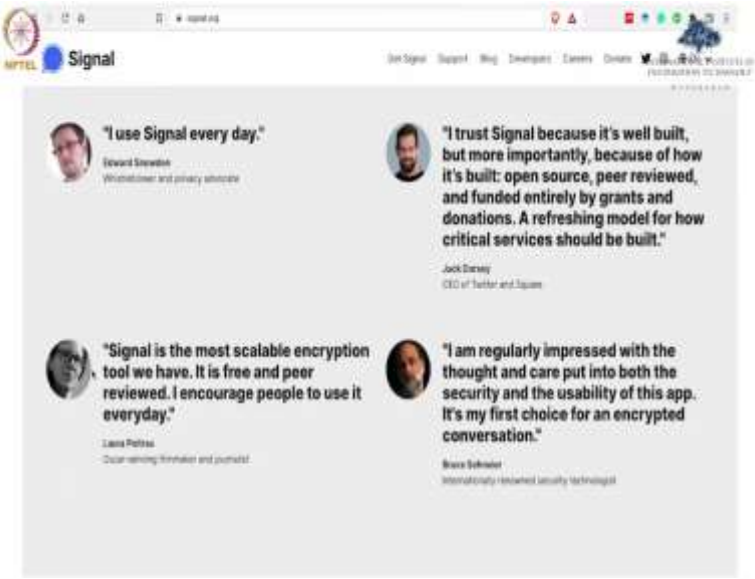


Instant Messengers (Hands-on)



Speak Freely

Say "hello" to a different messaging experience. An unexpected focus on privacy, combined with all of the features you expect.



"I use Signal every day."

Edward Snowden
Whistleblower and privacy advocate

"I trust Signal because it's well built, but more importantly, because of how it's built: open source, peer reviewed, and funded entirely by grants and donations. A refreshing model for how critical services should be built."

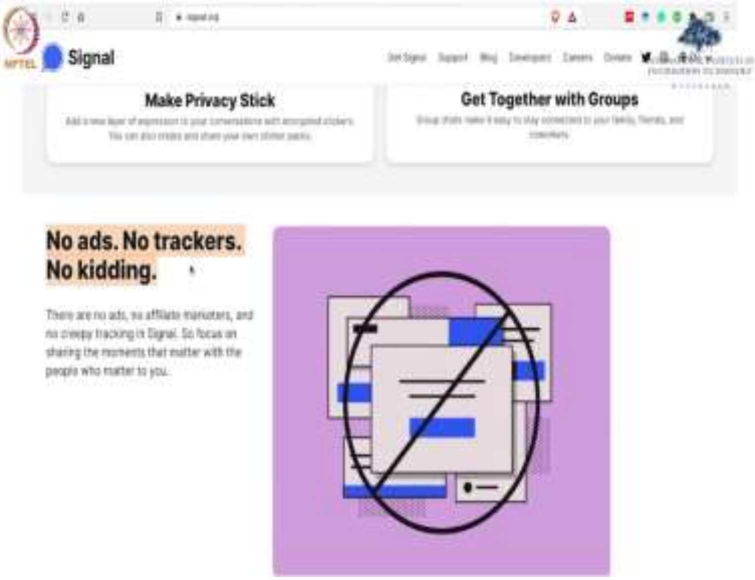
Jack Dorsey
CEO of Twitter and Square

"Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday."

Laura Poitras
Oscar-winning filmmaker and journalist

"I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation."

Bruce Schneier
Internationally renowned security technologist



Make Privacy Stick

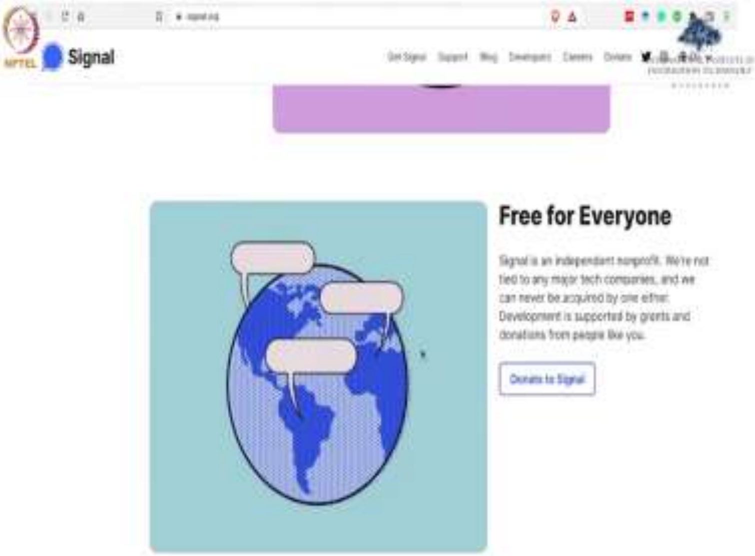
Add a new layer of expression to your conversations with encrypted stickers. You can also create and share your own sticker packs.

Get Together with Groups

Group chats make it easy to stay connected to your family, friends, and coworkers.

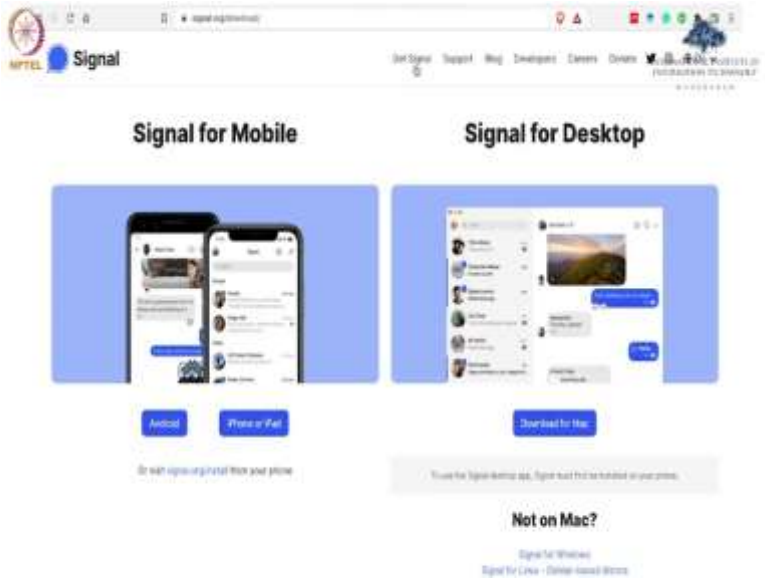
No ads. No trackers. No kidding.

There are no ads, no affiliate marketers, and no creepy tracking in Signal. So focus on sharing the moments that matter with the people who matter to you.



Free for Everyone

Signal is an independent nonprofit. We're not tied to any major tech companies, and we can never be acquired by one either. Development is supported by grants and donations from people like you.



Signal for Mobile

Signal for Desktop

Not on Mac?

Signal for Windows

Signal for Linux - Debian-based distros

Now let us have a look at another next section of this tutorial, which is instant messengers with encryption. So, there are 3 instant managers a lot more, but we will discuss about signal, Wire, and Ricochet, 3 instant messengers with encryption. Let us have a look at the signal home.

So, you might have came across this secure messaging app signal during COVID 19 pandemic times when suddenly WhatsApp and other messaging apps, they changed their policy and there was huge discussion over the social media platforms such as Twitter that we should download and use the signal apps and one of the prominent feature of this signal messaging app that it has an unexpected focus on privacy for the features that you combine that you want to use.

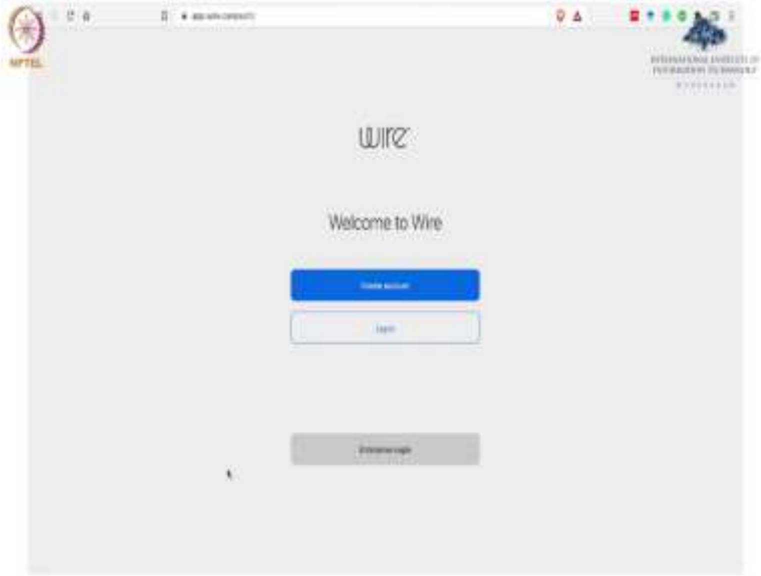
So, you can see here a lot of reviews that people have given for the signal app. And if you will see here that there are no ads, no trackers, no kidding, nothing. Privacy is the main that matters for the signal and it is a independent nonprofit organization where they do not have any tie up with the major tech companies. So, it only operates on the donation that it get from the, by crowdsourcing.

So, if you can download the signal app for Android, iPhone, and also you can download it for desktop, download for Mac, Windows, Linux and Debian based operating systems, so signal app is available. And if you will see the feature of this signal app it is the source is open code and it is (())(18:43) secure messaging and it is also protocol which was developed by an entrepreneur and cryptographer who is privacy enthusiast and activist Marlinspike.

And this is a pure app. So, this protocol is also being used by many other companies. And all the text messages, voice, video calls, these are protected using extended triple Diffie Hellman key agreement protocol.

So, such kind of algorithms are use and E2EE messaging protocol it use and it is available freely. You also have free version as well as well as you have some premium versions as well. But also there are some disadvantages. So, by disadvantages, we mean that there are limited support for some free users. And there is no 2-factor authentication that is present in the signal.

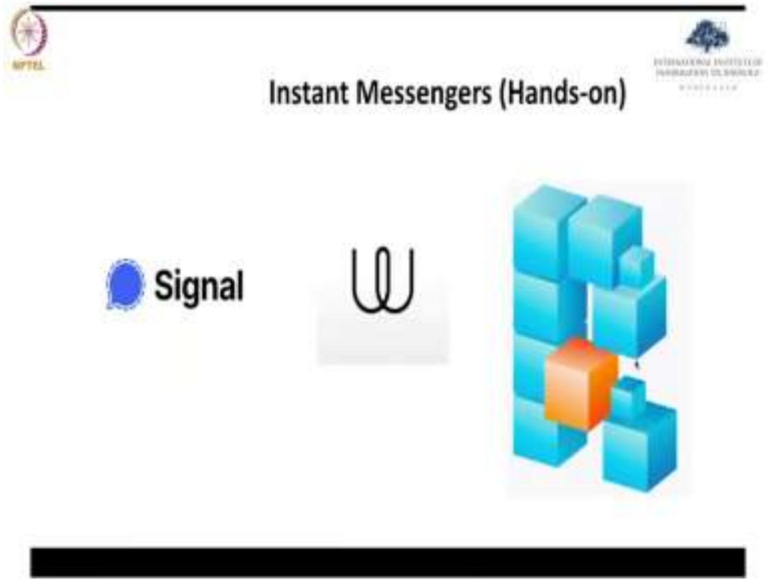
(Refer Slide Time: 19:52)



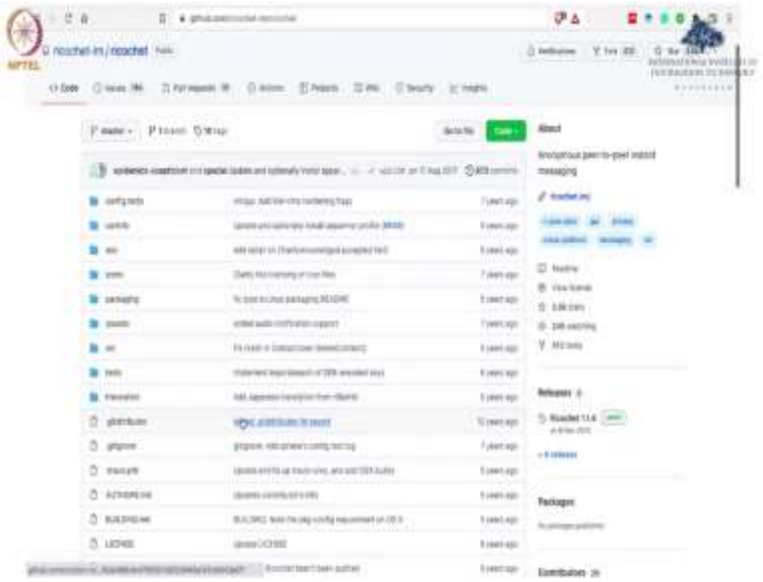
So, in order to incorporate some more secure video chat platform the wire is also one of the messaging app, messaging voice or video chat platform which is developed by the company of Switzerland and some supporters, some people they prefer wire over signal because it does not require any phone number, it does not require your phone number to registers, you can just pop to provide your phone number so that user can easily find you.

But it is not mandatory, you can totally use your disposable email address instead, so that it will only identify for you to identify yourself using your username and choose. So, this wire, platform is also one the most, wire messaging app is also one of the most secure app encryption-based app that is present.

(Refer Slide Time: 20:53)



Instant Messengers (Hands-on)



ricochet-im / ricochet Public

config.tests	[illegible]	7 years ago
contrib	[illegible]	5 years ago
doc	[illegible]	5 years ago
icons	[illegible]	7 years ago
packaging	[illegible]	5 years ago
sounds	[illegible]	7 years ago
src	[illegible]	5 years ago
tests	[illegible]	6 years ago
translation	[illegible]	5 years ago
.gitattributes	[illegible]	10 years ago
.gitignore	[illegible]	7 years ago
.travis.yml	[illegible]	5 years ago
AUTHORS.md	[illegible]	5 years ago
BUILDING.md	[illegible]	5 years ago
LICENSE	[illegible]	8 years ago

About

Anonymous peer-to-peer instant messaging

Readme

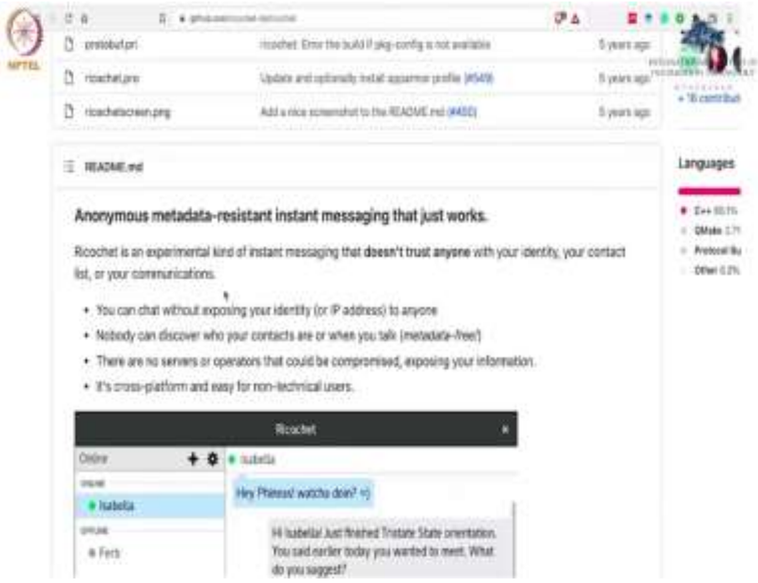
View license

Releases

Ricochet 1.1.4

Packages

Contributors



protobuf.pri	ricochet: Error the build if pkg-config is not available	5 years ago
ricochet.pro	Update and optionally install apparmor profile (#549)	5 years ago
ricochetscreen.png	Add a nice screenshot to the README.md (#432)	5 years ago

README.md

Anonymous metadata-resistant instant messaging that just works.

Ricochet is an experimental kind of instant messaging that **doesn't trust anyone** with your identity, your contact list, or your communications.

- You can chat without exposing your identity (or IP address) to anyone
- Nobody can discover who your contacts are or when you talk (metadata-free!)
- There are no servers or operators that could be compromised, exposing your information.
- It's cross-platform and easy for non-technical users.

Hey Phineas! watcha doin? =)

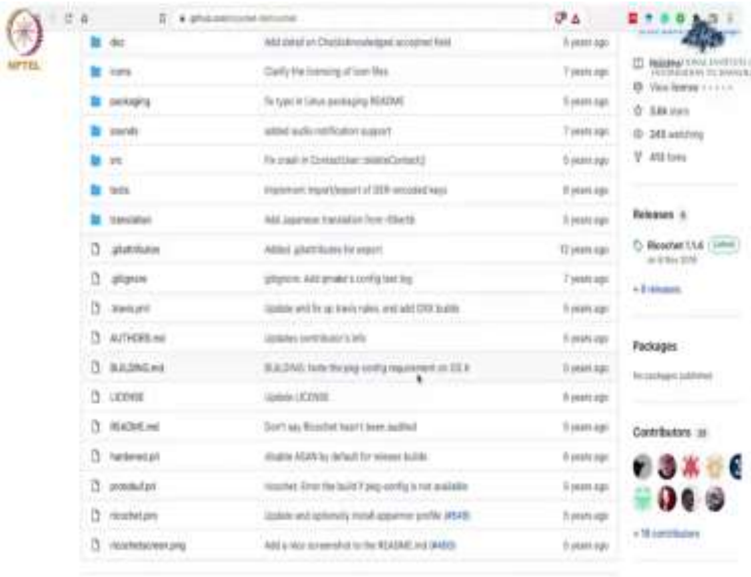
Hi Isabella! Just finished Tristate State orientation. You said earlier today you wanted to meet. What do you suggest?

Next is next is you can see on the third, the third figure here, which is Ricochet. So, Ricochet is also a messaging platform, I can show you the GitHub of Ricochet, it is a messaging platform, but how it is different from the other two is that it is based on Tor secure network. So, therefore, you can have your messages completely anonymous over the platform. So, user security and anonymity both are maintained at the same time and there is no central server where it stores data.

So, you can chat without exposing your identity or IP address. No one can discover who your contacts and what you talk about metadata free which is called as there are no servers or operators exposing any information. And it is cross platforms are easy for other non-technical users to use it widely.

So, if you truly want anonymity on internet, then Tor is always a best and this Ricochet pro's platform desktop (())(22:02) manager it allows you for anonymous communication via Tor. So, great privacy is there and there is zero need to trust anybody. So, this is one of the important feature. And if I talk about encryption, it uses and complex encryption scheme despite numerous high level of attacks, few which have some good limited success. So, torr always remain highly secure.

(Refer Slide Time: 22:38)



doc	Add detail on ChatAcknowledged accepted field	5 years ago
icons	Clarify the licensing of icon files	7 years ago
packaging	Fix typo in Linux packaging README	5 years ago
sounds	added audio notification support	7 years ago
src	Fix crash in ContactUser::deleteContact()	5 years ago
tests	Implement import/export of DER-encoded keys	8 years ago
translation	Add Japanese translation from Transifex	5 years ago
.gitattributes	Added .gitattributes for export	10 years ago
.gitignore	gitignore: Add qmake's config test log	7 years ago
.travis.yml	Update and fix up travis rules, and add OSX builds	5 years ago
AUTHORS.md	Updates contributor's info	5 years ago
BUILDING.md	BUILDING: Note the pkg-config requirement on OS X	5 years ago
LICENSE	Update LICENSE	8 years ago
README.md	Don't say Ricochet hasn't been audited	5 years ago
hardened.pri	disable ASAN by default for release builds	6 years ago
protobuf.pri	ricochet: Error the build if pkg-config is not available	5 years ago
ricochet.pro	Update and optionally install apparmor profile (#548)	5 years ago
ricochetscreen.png	Add a nice screenshot to the README.md (#480)	5 years ago

Readme

View license

3.4k stars

245 watching

410 forks

Releases 8

Ricochet 1.1.4 Latest

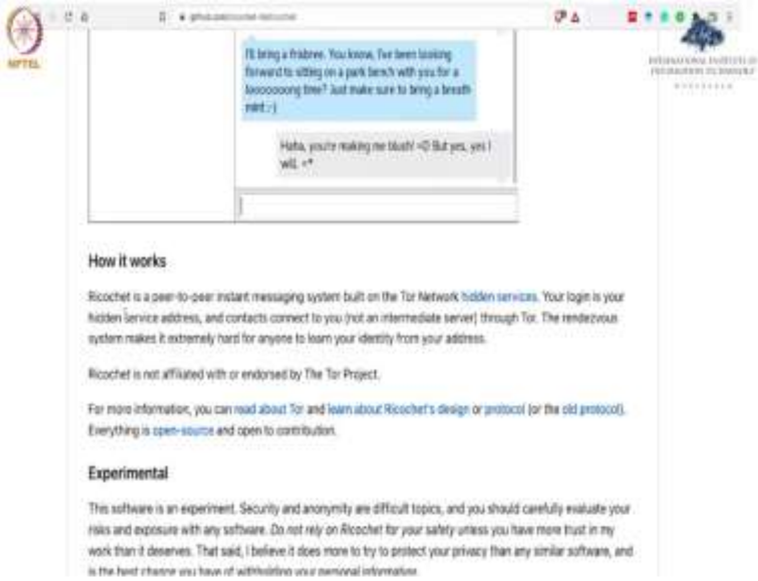
+ 8 releases

Packages

No packages published

Contributors 28

+ 18 contributors



I'll bring a frisbee. You know, I've been looking forward to sitting on a park bench with you for a looooooong time? Just make sure to bring a breath mint :-)

Haha, you're making me blush! <3 But yes, yes I will. <*

How it works

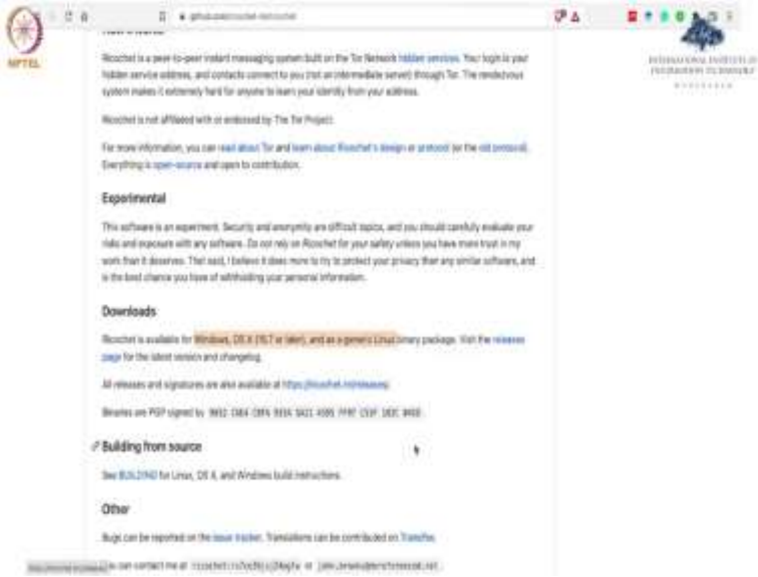
Ricochet is a peer-to-peer instant messaging system built on the Tor Network hidden services. Your login is your hidden service address, and contacts connect to you (not an intermediate server) through Tor. The rendezvous system makes it extremely hard for anyone to learn your identity from your address.

Ricochet is not affiliated with or endorsed by The Tor Project.

For more information, you can read about Tor and learn about Ricochet's design or protocol (or the old protocol). Everything is open-source and open to contribution.

Experimental

This software is an experiment. Security and anonymity are difficult topics, and you should carefully evaluate your risks and exposure with any software. *Do not rely on Ricochet for your safety unless you have more trust in my work than it deserves.* That said, I believe it does more to try to protect your privacy than any similar software, and is the best chance you have of withholding your personal information.



Ricochet is a peer-to-peer instant messaging system built on the Tor Network hidden services. Your login is your hidden service address, and contacts connect to you (not an intermediate server) through Tor. The rendezvous system makes it extremely hard for anyone to learn your identity from your address.

Ricochet is not affiliated with or endorsed by The Tor Project.

For more information, you can read about Tor and learn about Ricochet's design or protocol (or the old protocol). Everything is open-source and open to contribution.

Experimental

This software is an experiment. Security and anonymity are difficult topics, and you should carefully evaluate your risks and exposure with any software. *Do not rely on Ricochet for your safety unless you have more trust in my work than it deserves.* That said, I believe it does more to try to protect your privacy than any similar software, and is the best chance you have of withholding your personal information.

Downloads

Ricochet is available for Windows, OS X (10.7 or later), and as a generic Linux binary package. Visit the releases page for the latest version and changelog.

All releases and signatures are also available at https://ricochet.im/releases/.

Binaries are PGP signed by `9032 CAE4 CBFA 933A 5A21 45D5 FF97 C53F 183C 045D`.

Building from source

See BUILDING for Linux, OS X, and Windows build instructions.

Other

Bugs can be reported on the issue tracker. Translations can be contributed on Transifex.

You can contact me at `ricochet:rs7ce36jsj24ogfw` or `john.brooks@dereferenced.net`.

So, you can explore the GitHub and these are the links, it is desktop app or you can install it from here, you can see here how these works. It is a peer to peer instant and open-source code is present then it is available for all these systems, Windows, OS X and Linux also.

So, you can build from source code for lender documentation. I hope this information would have helped you to safeguard your privacy online so there are more instant messengers and password managers as well. But these are the prominent ones that seems very handy and easy to use. Thank you.