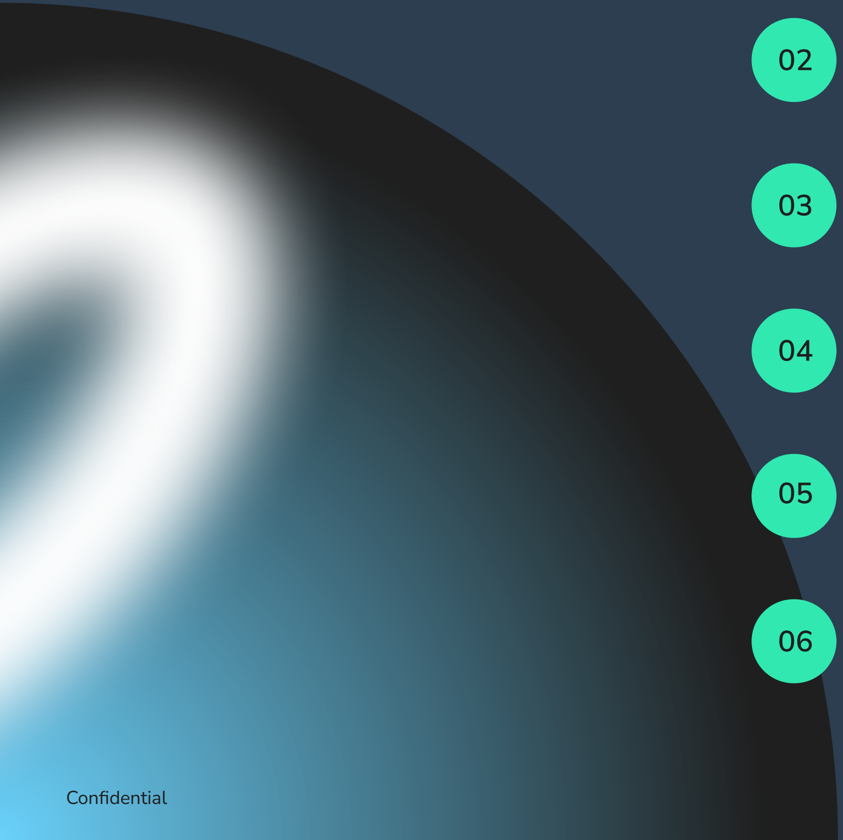
DEXIT PRESENTS

The Secret Life of Passwords: Past, Present & Future

Overview



01 The origins of passwords

02 The Password Problem We All Share

03 Passwords Go Public

04 Updating Passwords to Passkeys

05 The Rise of Encryption & Hashing

06 Password Alternatives Emerging

The Origin of Passwords

1960s: First computer password at MIT (Compatible Time-Sharing System).

Purpose: Keep personal files private — not protect against hackers!

Alternatives were personal data

WHat is your mother’s maiden Name?

What street did you grow up on?

Who was your favorite pet?

First Hacker

Allan Scheer

Before WW2

In fact, Ali Baba and the Romans used passwords to confirm the identity of the person bringing them news.

The Password Problem We All Share…

- “How many passwords do you have… and how many do you *actually* remember?”
- Brief audience poll or show fun stats (e.g., *the average person has over 255 passwords!*).
- “Let’s see how we got into this mess…”

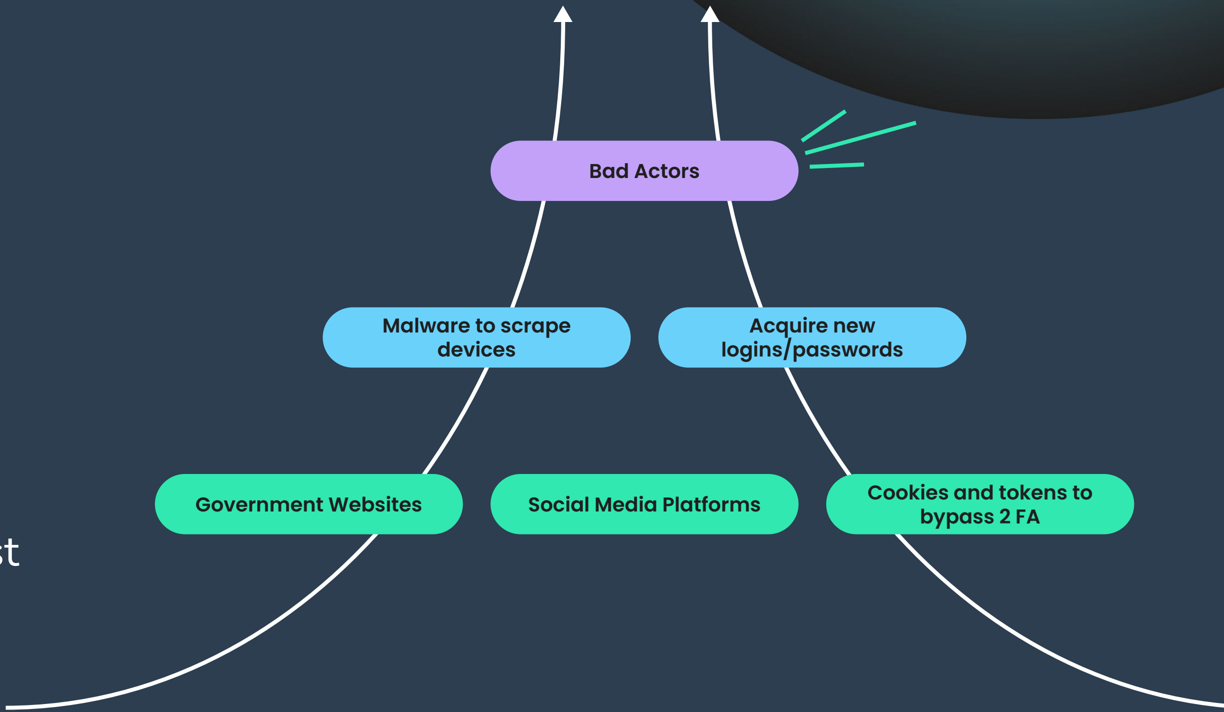
POLL: How many people in the webinar use a third party service to help them remember their passwords?

Passwords go Public

Databreaches and Hackers are commonplace today.

What’s new is the VOLUME of data that is being stolen and where they are stealing it from.

2025- The largest password heist happened in June this year, stealing over 16 BILLION user passwords and logins.


Bad Actors
Malware to scrape devices
Acquire new logins/passwords
Government Websites
Social Media Platforms
Cookies and tokens to bypass 2 FA

Breaking 2 FA barriers

How a bad actor might get around 2 FA

Introduce your audience persona, who they are, and where they come from. Mention their age and profession.

Leaked Cookies and session tokens

Leaked cookies and session tokens could be used to break into accounts with weaker 2FA. If your account doesn't reset cookies after you change your password, they might be able to trick the 2FA system into thinking they've provided the proper 2FA code or credential

Phishing Schemes

Hackers can use your password to trigger a 2FA code generation.

WHen you get the code texted to your phone, they will trick you into giving them the code.

You've been victimized

Once they can try to trick you into handing it over, potentially posing as the company behind the account in question.

If and when you send the code, they'll gain access your account.

Passwords are NOT Pass keys
What are Passkeys?

NordPass

KEEPER

RoboForm

LastPass

1Password

Proton Pass

Passwords	Passkeys
Tied to the account	Tied to a device or third party manager
Log in credentials can be stolen / phished	Cannot be stolen or phished due to device ownership
Considered old technology	May include a 4 digit pass, facial recognition, and fingerprint.

Needs an AUTHENTICATOR:

-Mobile Device

Or Third party password manager app that supports passkeys

Let’s talk about Mobiles & Passkeys

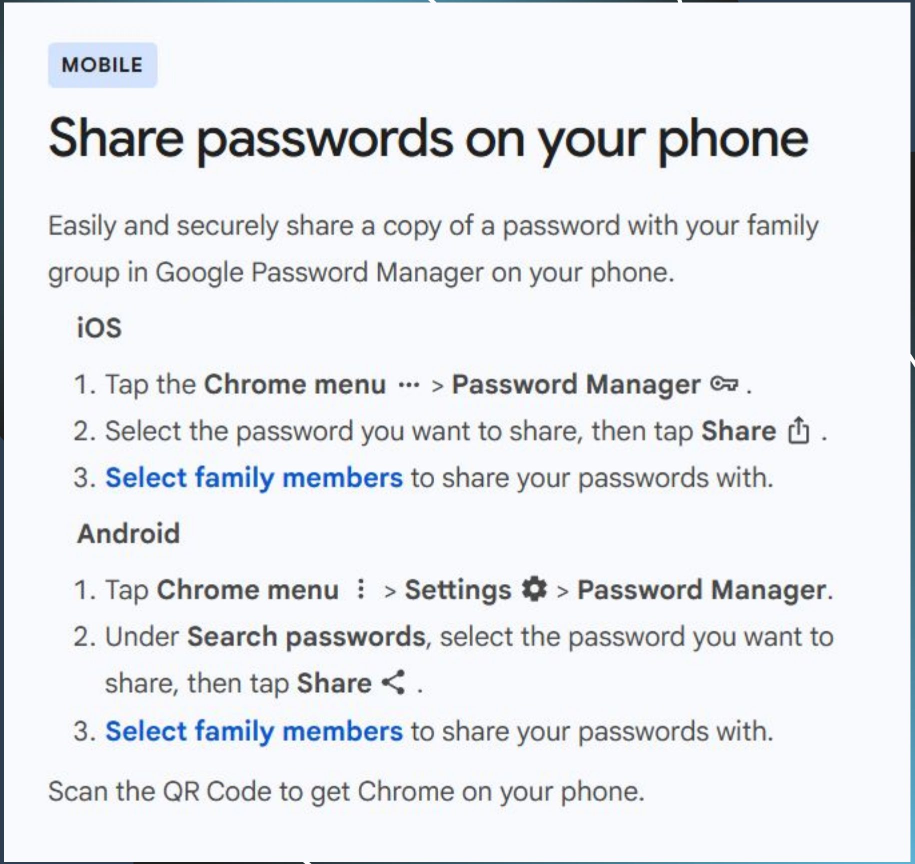
When you use passkeys on your Android device, they're stored in your Google Password Manager. Passkeys are securely backed up and synced between your Android devices. Create a passkey to simplify your sign in.

You can find and manage your passkeys in the Passwords app on your iPhone, iPad, or Mac. You can also find them by asking Siri.

Sharing Passwords

Knowing that passwords and passkeys are the gateway to your online life, sometimes it’s worth having a plan and conversation about these “digital padlocks” in case someone needs to access your account to help manage things.

Various companies have various policies and options when it comes to family sharing.



MOBILE

Share passwords on your phone

Easily and securely share a copy of a password with your family group in Google Password Manager on your phone.

iOS

1. Tap the **Chrome menu** ⋯ > **Password Manager** 🔑 .
2. Select the password you want to share, then tap **Share** ⇪ .
3. **Select family members** to share your passwords with.

Android

1. Tap **Chrome menu** ⋮ > **Settings** ⚙ > **Password Manager**.
2. Under **Search passwords**, select the password you want to share, then tap **Share** < .
3. **Select family members** to share your passwords with.

Scan the QR Code to get Chrome on your phone.

Next steps

Free Tech Guide

INVENTORY

Figure out what you have.
Do you have a google account? More that one?
Do you have an apple phone? Figure out where your stuff is.

MAKE A PLAN

List the companies where you have log ins, if you use a password bank, look into their passkeys.
You may want to set up a passkey program.

SHARE YOUR PLAN

Talk to your family members this Thanksgiving and make it known that you have a tech plan.
Let them know they are being added to accounts that matter, and that they will have access, so they need to be made aware.

Thank you!

If you have more questions:

dexit@dexitplan.com

Free Tech Guide