



Passwords-2FA-Passkeys

LLL 2025-03-10

George Saly

Recent News: February 2025

1. Feb 2024: Matthew Van Andel was hacked (Feb 2024) after downloading an AI-powered photo tool that contained hidden malware.
2. Jul 2024: The malware allowed hackers to access his personal and professional accounts, including his Disney login credentials.
3. Did he use “an **online** password manager”?
 - **YES:** the hackers were able to gain access to his password manager database **because he had not enabled two-factor authentication (2FA)** for the software.

Definitions:

- Disconnected from the network Secure
- Your 'Network' **AND** Your 'device' Less Secure
- Not Your 'Network' **OR** Not Your 'device' Insecure
 - Password Theft and more.
 - Avoid personal transactions!
 - Hotel Network, Coffee Shop, Hotel computer, Friend Computer

Time to crack Passwords with a computer

		Crack Time	
<i>Characters</i>	<i>Upper</i>	<i>Upper & Lower</i>	<i>Upper & Lower & Number</i>
8	Minutes	Days	Months
12	Days	Months	Decades
20	37M Years		

Accessing bank at the **branch**

1. Present Bank Card [ID]
2. Enter PIN [*Password*]
3. Transaction? *Not Yet*
4. Present Picture ID [*2FA - 2nd Factor for Authentication*]
5. Transaction? =====> YES

2FA has been around forever !

Roman Military Camp:

1. Tessera: wooden tablet identifies soldier as part of group.
2. Soldier recites correct password or phrase for the day.

We are using 2FA in our daily lives :

Safety Deposit Box: My key and Bank Key

Health: Health Card + Photo ID

Let's also use it on our Online lives.

Accessing Bank ONLINE

1. Type in ID [ID] Insecure
2. Type in Password [Password] Not Secure
3. Transaction? _____
4. Get Text/Phone Call/Push/email [2FA] More Secure
5. Transaction? =====> Proceed

[Password (encrypted) stored in 2 locations: your device and server]

Complex Passwords => Password Manager

Benefits

- Do not have to remember password, particularly complex ones.
- Auto-fills login & password into web form
- May have link to website

Password Manager - Roll your own

- Spreadsheet / Editor : Enter Site URL, Login, Password from generator.
 - <https://bitwarden.com/password-generator/#password-generator>
 - Encrypt it (Excel, Numbers, not Sheets).
 - Back it up (a usb stick, printout) and store it at home.
 - Save the Encryption password in a separate location.
- Booklet and Ink: Website, Date, Time, Login, Password

BIOMETRICS - Fingerprints



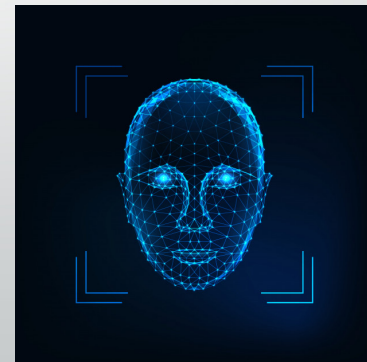
Applies to current smartphones <3 years old

- Identical Twins : Different
- Fingerprints
 - Unique 1 in 64 billion
 - False Acceptance Rate (FAR): Likelihood of an unauthorized person being granted access as low as 1 in 50,000 (Mechanical car keys : 1 in 20,000).
 - False Rejection Rate (FRR): Likelihood of a legitimate user being denied access is around 2%.

BIOMETRICS - Facial Recognition

Applies to current smartphones <3 years old

- Identical Twins : Fails - Cannot distinguish
- Apple FaceID : Robust
 - FAR and FRR : 1 in 1,000,000
 - 3D scanning technology
- Android:
 - Weak, not for banking, OK for logging in.
 - 2D scanning technology



PASSKEY

- Passkey is an encrypted combination of a special password and biometric data.
 - Stored on your phone, not on a server.
 - Use a 2FA mechanism.
 - Prove your identity for a SINGLE site.
 - Try it gradually, one site at a time:
 1. Uber
 2. Amazon
 3. Google, Apple, Microsoft,
- *Very difficult to tell, email, text or ask for a Passkey!*



Never, Ever .. Tell, Email, Text..

- **PASSWORD**
- **2FA code**

- 
- Upgrade to 2FA **Takeaway**
 - Complex passwords + password manager
 - Play with Passkey: it's the future.