



Smartphone Security – What to Watch For



Presented by
Dr. Milan Frankl, MBA, PhD.
Emeritus Professor
Business & Computer Science



Topics Covered

- Why Hackers want your Personal Information
- What do we use our smartphone for?
- How many applications (APs) do you have on your smartphone?
- Smartphone Battery Myths
- Several Ways to Hack a Smartphone
- Breaking in via Cookies
- Breaking in via Bluetooth
- Man-in-the-Middle Wi-Fi attacks (Spoofing)
- Spoofing Examples
- Phishing
- Phishing Attempts
- Web Browsers
- Password Strength
- Are Passwords Dead?
- Hardware Authentication Devices
- Mobile Security Software
- Extreme Examples of Privacy Breaches
- They've broken in, now what?
- Support in Fighting Scams
- Recovering from Internet, Email, and Telephone Scams
- Additional References
- Questions



Why do hackers want your PII?

What are hackers looking for?



shutterstock.com #19058278

How can hackers monetize their objectives?

By collecting PII

(Personally Identifiable Information)



PII is information that criminals are trying to obtain to commit fraud, identity theft, and other financially damaging crimes.

- **Hackers can sell your data to other criminals**
- **Stolen personal information is fuel for identity theft**
- **Login details are needed for account takeover**
- **Stolen data is used to target phishing attacks and extortion**
- **Stolen personal information can be used to harm companies**

<https://www.f-secure.com/en/home/articles/why-do-hackers-want-your-personal-information>



What do we use our smartphones for?

- **Texting (88%)**
- **Email (70%)**
- **Facebook (62%)**
- **Camera (61%)**
- **Reading News (58%)**
- **Online Shopping (56%)**
- **Checking the Weather (54%)**
- **WhatsApp (51%)**
- **Banking (45%)**
- **YouTube (42%)**



ComputerHope.com

Phone calls don't even make the top ten, coming in at number 11 with just 41% of people using this feature regularly.

<https://turbofuture.com/cell-phones/Disadvantages-of-Mobile-Phones>



How many Applications (Apps) do you have on your smartphone?

- **Take out your smartphone**

Go to “settings” and page down. It will display the number of Apps on your phone.

Normally, an average person has **40 apps** installed on the smartphone. Out of that 40 apps, 90% of the time is split between 18 apps. This means, more than half of those apps remain unused.

• Music	Gaana, Saavn, Spotify, Prime Music
• Reading	Kindle, Libby, ReadEra, Epub Reader, Audible, Aldiko, WordPress, Wattpad
• Payment	PayTM, Mobikwik, Freecharge, Google Pay
• Shopping	Flipkart, Amazon, Jabong, Myntra, eBay, OLX, Quikr
• Gaming	PUBG, Angry Birds, Subway Surfers, Temple Run, 2048
• Photo	PicsArt, Pixlr, Snapseed, PhotoGrid, Google Photos
• Learning	Udemy, Coursera, Udacity, StupidSid
• Social Networking	WhatsApp, Hike, Facebook, LinkedIn, Snapchat, Instagram, Twitter, Tumblr
• Streaming	Netflix, Amazon Prime, Hotstar, SonyLIV, Zee5, Viu, Voot, Popcorn
• Bookings	BookMyShow, Inox, PVR, Carnival Cinemas, Cinépolis
• Travel	Ola, Über, mIndicator, OYO, Thrillophilia, MakeMyTrip, IRCTC, Goibibo, Trivago
• Food	Swiggy, Zomato, Über Eats, FoodPanda, Scootsy, DineOut, Eatigo
• Google Apps	Maps, Translate, Docs, Sheets, Slides, Allo, Hangouts, Photos, PlayStore, Lens
• Bundled System Apps	clock, calendar, calculator, contacts, camera, gallery, messages, settings, weather
• Utility and Productivity Apps	IFTTT, Smart Tools, Reddit, TickTick, Otter Voice Meeting Notes, SwiftKey Keyboard.



Smartphone Battery Myths

- Go to **SETTINGS** and scroll down to **BATTERY**. What do you notice?
 - **Myth #1 Smartphone batteries are made to last forever.**
 - *The lithium-ion batteries found in most smartphones today are expected to maintain at least 80% of their original capacity for around 300 to 500 full charge cycles. (About 2 years)*
 - **Myth #2: It doesn't matter when or how long you charge your smartphone battery.**
 - *Rule of Thumb: To get your smartphone battery to last the longest, charge it to 80% and recharge it when it hits 20% to avoid stressing the system.*
 - **Myth #3: It's terrible to let your phone die.**
 - *If you want your battery to stretch its legs a bit every now and again, it is okay to let it run a "full charge cycle," or to let it die and then charge back up to 100% again. This helps the little computers that control the battery remember where its high and low points are and will give you a more accurate reading of your charge.*
 - **Myth #4: All chargers are basically the same.**
 - *Reputable third-party chargers are fine, but that cheap-o do-it-all charger you got from the gas station might not be. Poorly-made chargers might provide too little or — and this is the scary one — too much power for your gadget to handle.*
 - **Myth #5: If your battery's dying, you have too many Apps running.**
 - *By closing the App, you also take it off the phone's short-term memory list. So the next time you need it, it has to load it back up again from scratch. All of that loading and unloading puts more stress on your device than just leaving it alone.*
- *Of course, there are exceptions to every rule*

<https://www.usatoday.com/story/tech/columnist/2017/04/02/smartphone-battery-myths-need-die/99852532/>



Several Ways to Hack a Smartphone

- Social Engineering
- Malvertising
- Smishing
- Malware
- Virus
- Worms
- Trojans
- Spyware
- Adware
- Ransomware
- Pretexting



Pretexting 101

Pretexting is a form of social engineering whereby a cybercriminal stages a scenario that baits victims into providing valuable information that they wouldn't otherwise.

- 

1. A fraudster **impersonates a trusted authority** and crafts a scenario to reach out to their victims.
- 

2. The victim **believes the scenario** and shares any information the 'trusted' authority requests.
- 

3. The fraudster **gains valuable information** from their victim and often uses it maliciously.



Breaking-in via Cookies



What is a computer cookie

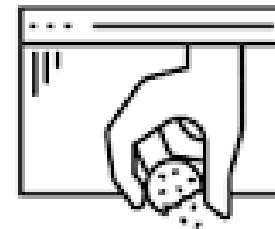
- A computer cookie, also known as an HTTP cookie, internet cookie, web cookie, or browser cookie, is text-string data your browser stores on your device.

Main type of cookies

- Session cookies (temporary)
- Persistent cookies (permanent – PWD, UID)
- First-party cookies (customer analytics)
- Third-party cookies (behaviour & demographics)
- Flash cookies (can hold up to 100KB of information)
- Zombies cookies (potential malicious software)

How to protect yourself from cookie stealing

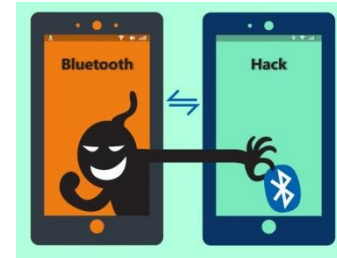
- Delete your cookies
- Use HTTPS connections
- Avoid using unprotected Wi-Fi connections
- Use a VPN (Virtual Private Network) \$\$\$



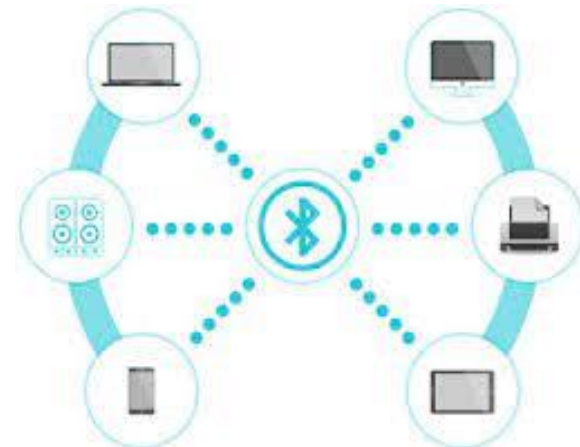
WEBSITE
COOKIES

Breaking-in via Bluetooth

- **Bluesnarfing:** Stealing info
-
- **Bluebugging:** Accessing the device
- **Bluejacking:** Sending anon info



Is your Bluetooth on? - Why?



Man-in-the-Middle Wi-Fi Attacks (Spoofing)

- **What:** disguising an email address, displaying a name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source.

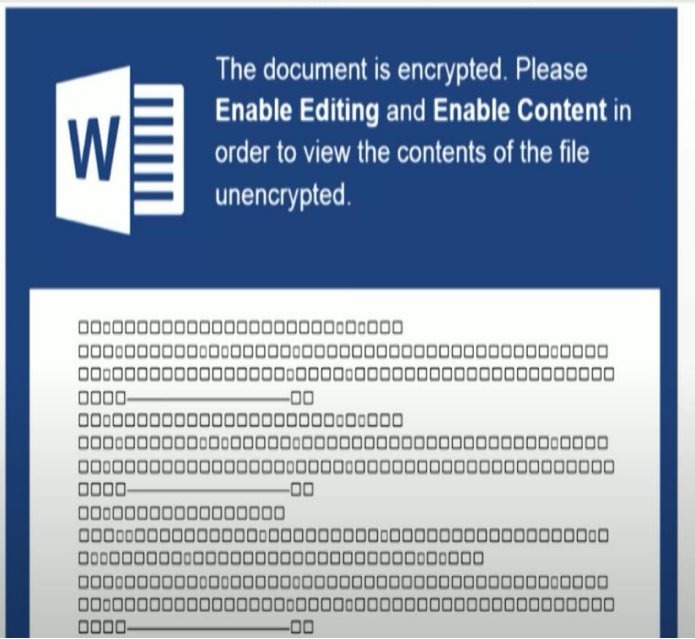
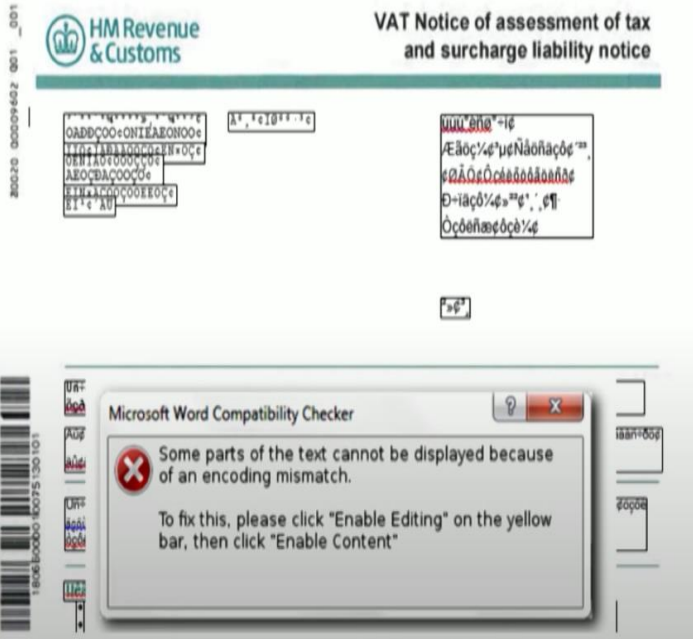


Avoiding spoofing: beware of unknown sources. [i.e. do not answer/click]

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Spoofting Examples

- **Avoiding spoofing: beware of unknown sources. [i.e. do not answer/click]**



<https://softwarelab.org/what-is-spoofing/#:~:text=In%20its%20most%20primitive%20form,a%20victim%20of%20phone%20spoofing.>



Phishing

- **Hacker sends a fraudulent (spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to deploy malicious software on the victim's infrastructure like ransomware.**
 - Exceptionally good deals or offers.
 - Unknown or unusual senders.
 - Hyperlinks and attachments.
 - Incorrect spelling in the web address.
 - Immediate pop-ups.





Phishing Attempts

- **For example, phishing attempts may:**
 - Say they've noticed suspicious activity or log-in attempts on your account
 - Claim there's a problem with your account or payment information
 - Say you need to confirm or update personal information
 - Include a fake invoice
 - Ask you to click on a link to make a payment
 - Claim you're eligible to sign up for a government refund
 - Offer a coupon for free goods or services

Phishing emails example



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Web Browsers

- **Mobile web browsers are emerging attack targets for mobile devices.**





Visit the website below for the strengths and weaknesses of some of the above.

<https://www.lifewire.com/list-of-mobile-web-browsers-3486250>

Password Strength

- **A measure of the effectiveness of a password against guessing or brute-force attacks.**
- **The strength of a password is a function of length, complexity, and unpredictability.**
- How Long It Takes to Crack a Password with Brute Force Algorithm

	8 characters password	10 characters password	
Lowercase letters only	instantly	instantly	
+ 1 uppercase letter	half an hour	1 month	
+ 1 number	one hour	6 years	
+ 1 special symbol	one day	50 years	

Are Passwords Dead?

“Hackers don’t break in, they log in.”

- Passwords are the most common digital authentication method to log in to company systems—is rife with problems, from being an annoyance to posing a security risk.
- Technology vendors are now coming up with methods to allow access to systems that don't require passwords. Mass adoption of these techniques is not happening anytime soon and organizations are better off improving password policy, working to prevent phishing attacks, and patching vulnerable software to secure their systems.
- Passwords are just not security and “password security” is no such thing. Passwords are well beyond their sell-by date. Last year, the top five passwords used in the USA, according to password manager Nordpass, were "123456", "123456789", "12345", "qwerty" and "password".
- Passwordless authentication is a type of multifactor method that replaces passwords with more-secure forms of identification such as biometric technology.



The image is a screenshot of a Microsoft advertisement. At the top left is the Microsoft logo. Below it is the text "milan.frankl1". The main headline reads "Break free from your passwords". Below the headline is a graphic showing a computer monitor displaying a Microsoft login page with a blue padlock icon, and a smartphone in the foreground showing a fingerprint scanner. Below the graphic, the text says "Get the smartphone app to sign in without a password. It's more convenient and more secure." At the bottom left is a link "No thanks" and at the bottom right is a blue button with the text "Get it now".

<https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-password-is-slowly-becoming-extinct.aspx>
<https://dgwbirch.substack.com/p/the-passing-of-passwords>
<https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/>

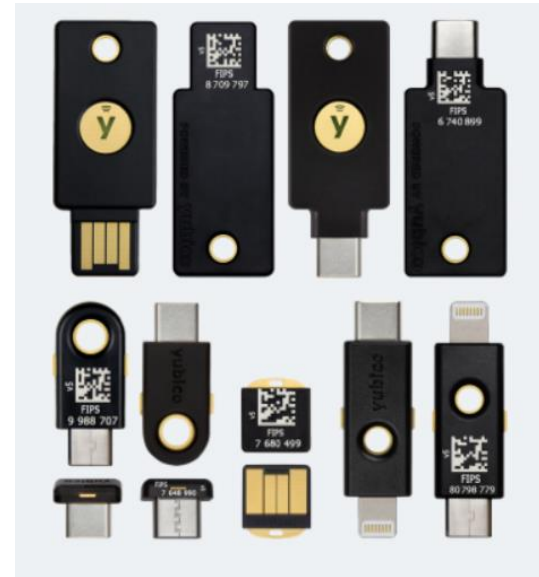


Hardware Authentication Devices

- **Hardware authentication devices protect access to computers, networks, and online services that support:**
 - **One-time passwords (OTP),**
 - **Public-key cryptography,**
 - **Authentication,**
 - **Universal 2nd Factor (U2F), and**
 - **FIDO2 protocols developed by the FIDO Alliance.**

(FIDO – Fast Identity Online)

<https://www.zdnet.com/article/best-security-key/>
<https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-public-key-cryptography>
<https://www.techtarget.com/searchsecurity/definition/authentication>
<https://www.techtarget.com/whatis/definition/Universal-2nd-Factor-U2F>
<https://www.techtarget.com/searchsecurity/definition/FIDO-Fast-Identity-Online>



Is there an alternative to YubiKey?

The best alternative is Authy, which is free.

<https://authy.com/>

Other great apps like YubiKey are andOTP, Nitrokey, Microsoft Authenticator and GNOME Authenticator.

<https://alternativeto.net/software/yubikey/>

Mobile Security Software

- **What Does Security Software Mean?**

A software that secures and protects a computer, network or any computing-enabled device. It manages access control, provides data protection, secures the system against viruses and network/Internet-based intrusions, and defends against other system-level security risks.

Examples for security software are as follows:





Extreme Examples of Privacy Breaches

- **Image Scanning**

Hypothetical Scenario (Child Rash)

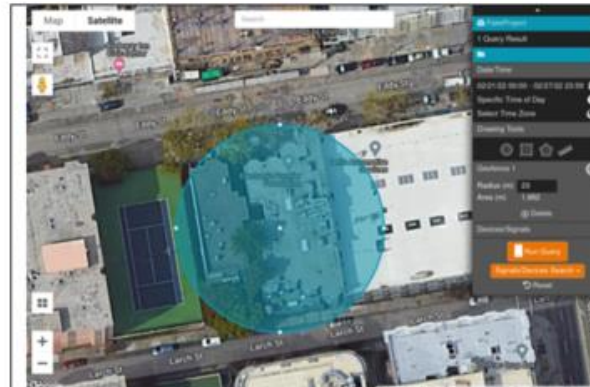
The Observer - Child protection - Google's image scanning illustrates how tech firms can penalize the innocent. (False Positive)



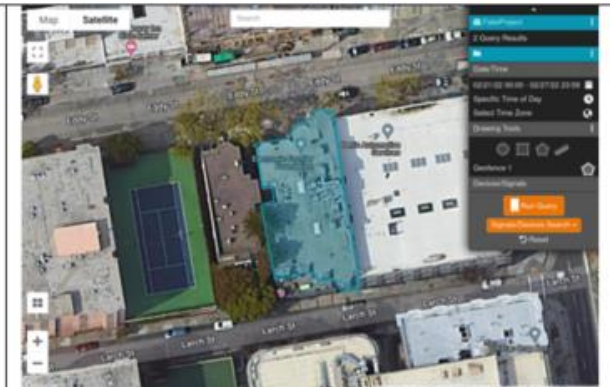
[https://www.theguardian.com/commentisfree/2022/sep/03/googles-image-scanning-illustrates-how-tech-firms-can-penalise-the-innocent?CMP=Share AndroidApp Other](https://www.theguardian.com/commentisfree/2022/sep/03/googles-image-scanning-illustrates-how-tech-firms-can-penalise-the-innocent?CMP=Share_AndroidApp_Other)

Extreme Examples of Privacy Breaches

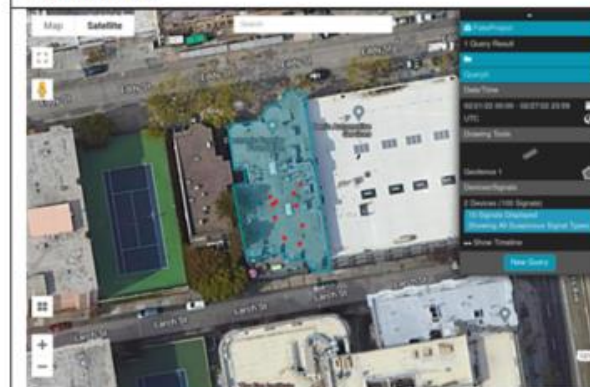
- Fog Reveal



Here, we've targeted the EFF offices in San Francisco.



We've now excluded EFF's neighbours, as well as our patio.



Our query results show 10 signals originating from 2 separate devices.



By grouping the signals by the device that produced them, Reveal can trace their path over time, giving us a view into how the device's owner was moving that day.



They've broken in, now what?

- **It depends - you may need to get help**
- **Government of Canada Scam Support**



<https://www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html>

So You've Been Pwned: What To Do When Your Private Data Goes Public

<https://www.pcmag.com/how-to/how-could-a-data-breach-affect-me>

- <https://haveibeenpwned.com/About>

';--have i been pwned?

Check if your email or phone is in a data breach



They've broken in, now what?

Opt-Out & Do Not Sell

Locate your mobile advertising identification number for your device:

iOS Device:

- Install "[The Identifiers](#)" **App** from the App Store
- Open the **App** to view your mobile advertising identifier (also called the IDFA on your iOS device)

Android Device:

- Install the "[Device Identifiers](#)" **App** from the Play Store
- Open the App to view your mobile advertising identifier (also called the AAID on your Android device)











Enter your mobile device advertising identifier and press 'Submit' to opt-out of our use and disclosure of your mobile location data. The opt-out is device-specific, which means that you need to opt-out separately for each of your mobile devices.

Do not Track

Google Analytics Opt-out Browser Add-on

Get Google Analytics Opt-out Browser Add-on

Available for Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge.

 IBA Opt-out (by Google) ★★★★★ 1,706	 Do Not Track ★★★★★ 123	 Protect My Choices ★★★★★ 292
 Cookie Killer for Facebook ★★★★★ 90	 Do Not Track ★★★★★ 4	
 HiddenTools for Google ... ★★★★★ 42	 Don't track me Google ★★★★★ 204	 TrustedSite ★★★★★ 97





Support in Fighting Scams

- Learn how you can protect yourself from scammers and be scam smart.
- **The Little Black Book of Scams**
[https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-IBBS2-EN.pdf/\\$file/CB-IBBS2-EN.pdf](https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-IBBS2-EN.pdf/$file/CB-IBBS2-EN.pdf)





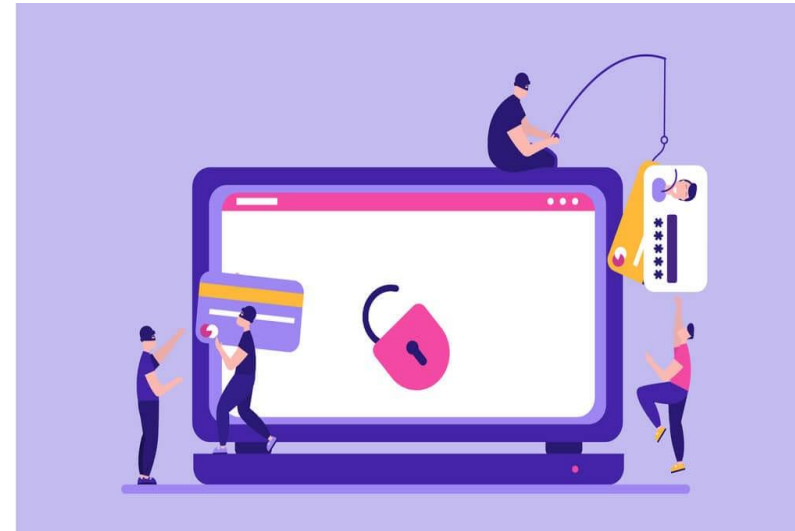
Recovering from the Internet, Email, and Telephone Scams

- **Recovering from Identity Theft**

<https://consumer.ftc.gov/features/identity-theft>

- **Ditching the smartphone**

<https://www.bbc.com/news/business-60067032>





Additional Readings & Videos

Suggested References Material

- How criminals are targeting investors on the Metaverse

<https://youtu.be/OFRGEEVxyWE>

- Recognize, Report, Recover

<https://fightcybercrime.org/>

Some useful websites

<https://www.computerworld.com/article/3239304/what-is-ifttt-how-to-use-if-this-then-that-services.html>

<https://support.ticktick.com/hc/en-us/articles/360011496412-3-Steps-to-Get-Started-with-TickTick>

<https://otter.ai>

https://play.google.com/store/apps?hl=en_CA&gl=US

<https://www.stites.com/resources/trademarkology/mobile-marking-trademarks-for-your-app-icon>

<https://www.f5.com/search?q=fraud>

<https://landing.google.com/advancedprotection/>

<https://fidoalliance.org/washington-examiner-farewell-passwords-how-passkeys-will-change-digital-privacy/>



Confused?

Before I came here I was confused about this subject.
Having listened to your lecture I am still confused.
But on a higher level.

[Enrico Fermi](#)



Thank You

- Questions

