

# Cyber Security: Game of Threats

امنیت سایبری: بازی با تهدیدات



## Digital Security Workshop

کارگاه امنیت دیجیتال

UNITED FOR  
IRAN اتحاد برای ایران

<https://united4iran.org>

Presenter

**Dawood Sajjadi**

PhD in Computer Science (UVic)  
Internet & Cyber Security Expert

<https://5tux.net>  
@5tuxnet

داود سجادی

دکترای علوم کامپیوتر

کارشناس اینترنت و امنیت سایبری

# Agenda

## 1. Brief Introduction

## 2. Cybersecurity Awareness

## 3. Smartphone Security

Physical Security  
Application Security  
Enable remote wipe  
Comms Security



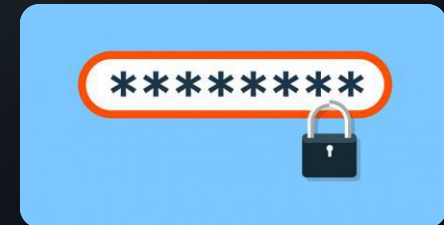
## 4. Online/Web Security

Secure Browsing  
Stay Anonymous  
Clean Social Media  
Backup Codes



## 5. Password Security

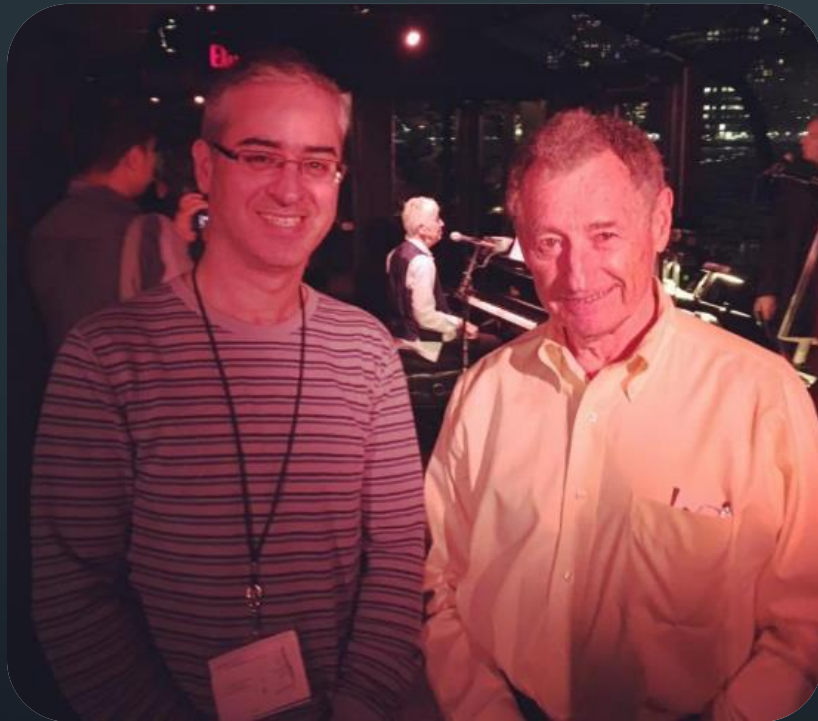
2-Factor Authentication  
Password Manager  
Sharing Passwords  
Passwordless Login



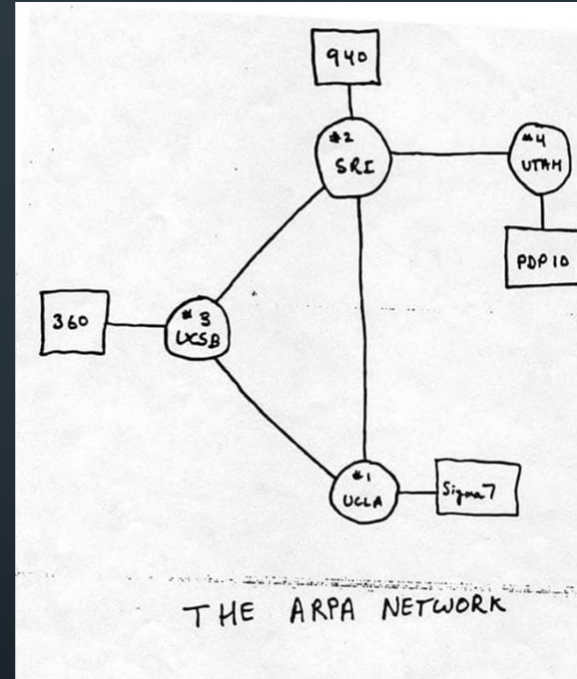
## 6. Recap & Conclusion

## 7. Questions & Answers (Q&A)

# The culture of the original Internet was **One of Trust.**



ACM Mobicom 2016, NYC

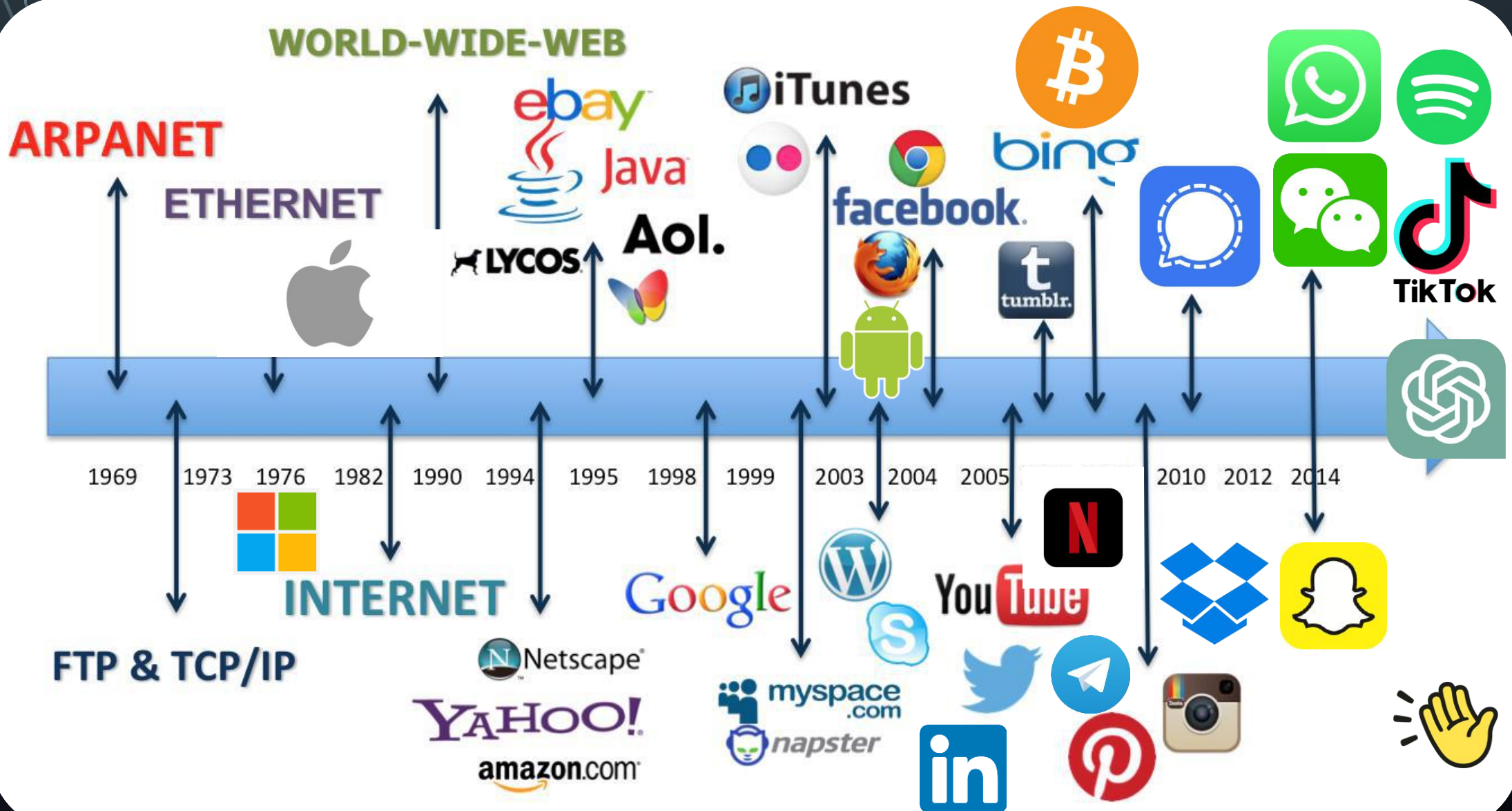


Leonard Kleinrock

**October 29th , 1969**

10:30pm, the first message transferred over the ARPANET  
UCLA → Stanford

# A Brief History of the Internet



شرکتها به دو دسته تقسیم می شوند



شرکتهایی که هک شده اند

و

شرکتهایی که هک خواهند شد

در نهایت همگی در یک دسته قرار خواهند گرفت و آنهایی که هک شده اند دوباره هک خواهند شد.

رییس اسبق پلیس فدرال آمریکا - رابرت مولر

# Cyber Awareness

Google Updates from Threat Analysis Group (TAG)

THREAT ANALYSIS GROUP

## Spyware vendors use 0-days and n-days against popular platforms

Mar 29, 2023 · 5 min read



dailymail.co.uk  
**Liz Truss's personal phone hacked by Putin's spies**

Eugene Kaspersky @e\_kaspersky · Jun 1  
We've discovered a new cyberattack against iOS called Triangulation. The attack starts with iMessage with a malicious attachment, which, using a number of vulnerabilities in iOS installs spyware. No user action is required.  
#IOSTriangulation  
[Show this thread](#)



rapid7.com

**RAPID7**

Blog Select TRY NOW

## Leaked Android Platform Certificates Create Risks for Users

Dec 02, 2022 | 1 min read | Erick Galinkin

Lookout

Identify and Prevent Threats with Lookout Threat Advisory

[Learn More](#)

[Back to Blog Home](#)

April 27, 2023 6 min read

## Lookout Discovers Android Spyware Tied to Iranian Police Targeting Minorities: BouldSpy

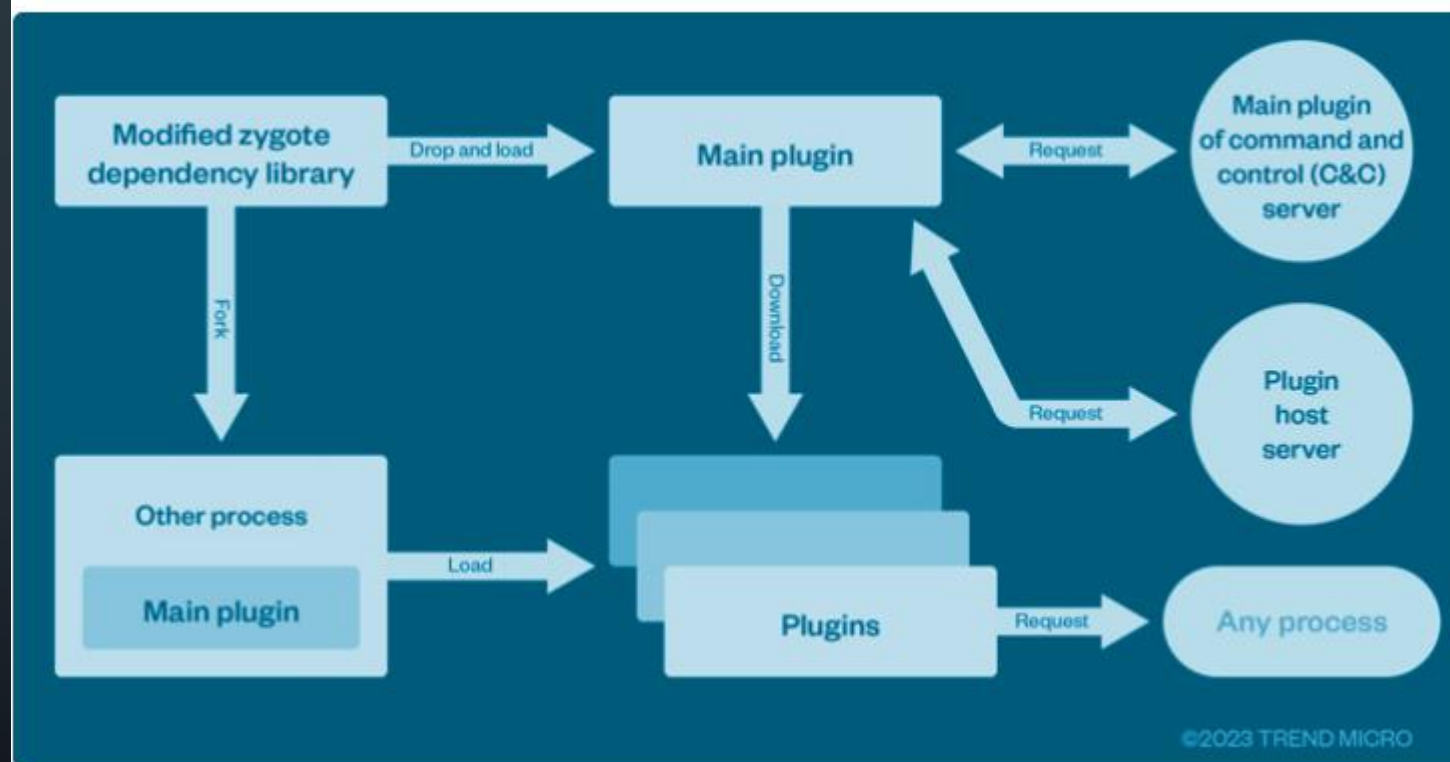
# Cyber Awareness

## QUADREAM FUNCTIONALITY

- Record audio from calls
- Record from the microphone (“hot mic”)
- Take pictures using front & back cameras
- Exfiltrate and remove keychain items
- Generate iCloud 2FA passwords
- Search through device files & databases
- Clean up its own traces
- Track location

## This Cybercrime Syndicate Pre-Infected Over 8.9 Million Android Phones Worldwide

May 18, 2023 Ravie Lakshmanan



A cybercrime enterprise known as **Lemon Group** is leveraging millions of pre-infected Android smartphones worldwide to carry out their malicious operations, posing significant supply chain risks.

# Phishing Smishing Vishing

Hackers try to  
manipulate people  
even using AI

آیا فرستنده پیام از شما **درخواست** انجام کاری دارد؟

آیا شما **فرستنده** پیام رو میشناسید؟

آیا شما **انتظار** دریافت چنین پیامی رو داشتید؟

آیا پیام قصد تحریک **عواطف** و احساسات شما رو دارد؟

Twitter/Instagram @5tuxnet  
داود سجادی



چهار نکته کلیدی جهت شناسایی پیامها  
و ایمیل‌های آلوده برای کلاه برداری

**درخواست**

**فرستنده**

تکنیک

**انتظار**

**عواطف**

**دفاع**

<https://www.instagram.com/reel/CnddAOCK3ui/?hl=en>



# Smart Phone Physical Security



Password for your  
Smartphone  
Screen Lock



Pattern  
Biometric  
Passcode



Infected  
Public  
Charging  
Stations



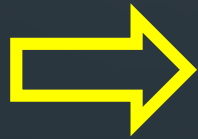
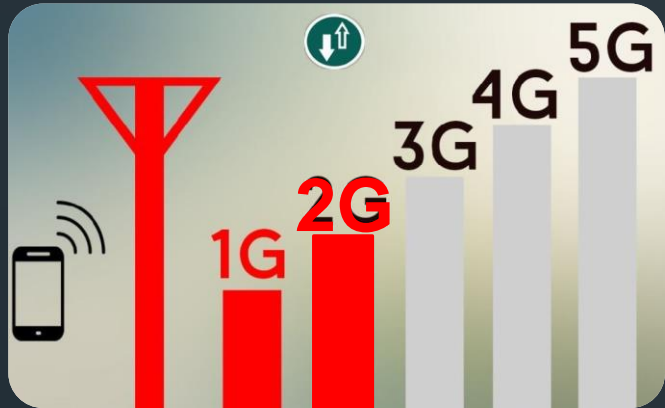
**USB data blocker**

# Smart Phone Physical Security

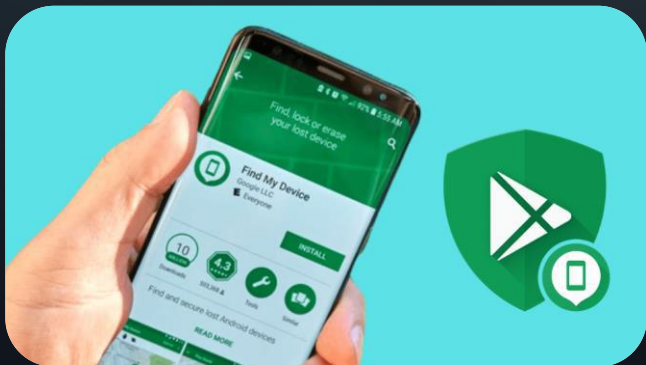
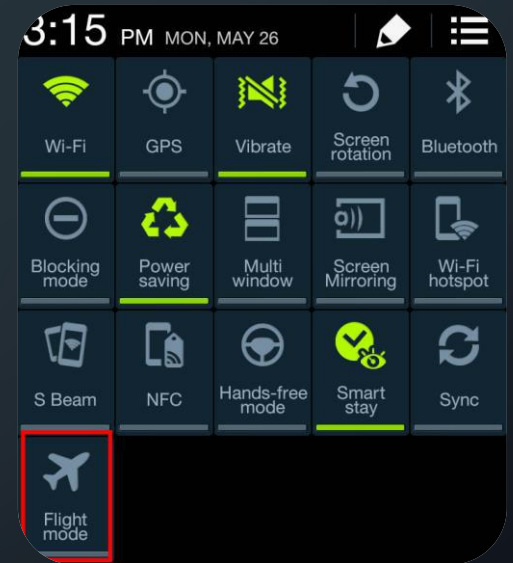
Infecting Computer and Phones via Only a USB Cable



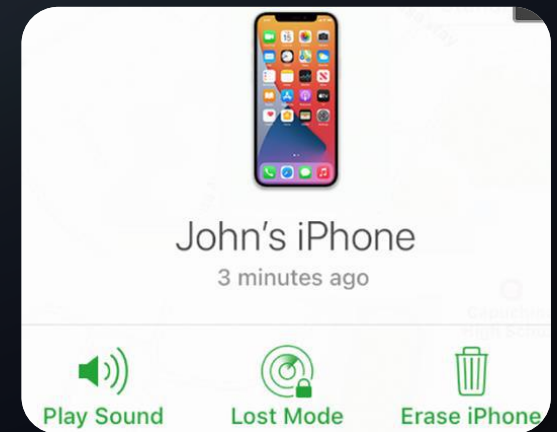
# Smart Phone Physical Security



Put your phone in Flight-mode and Disable Bluetooth to Reduce your Wireless Footprint



Enable Remote Wipe (Erase) for your phone and know how to do it

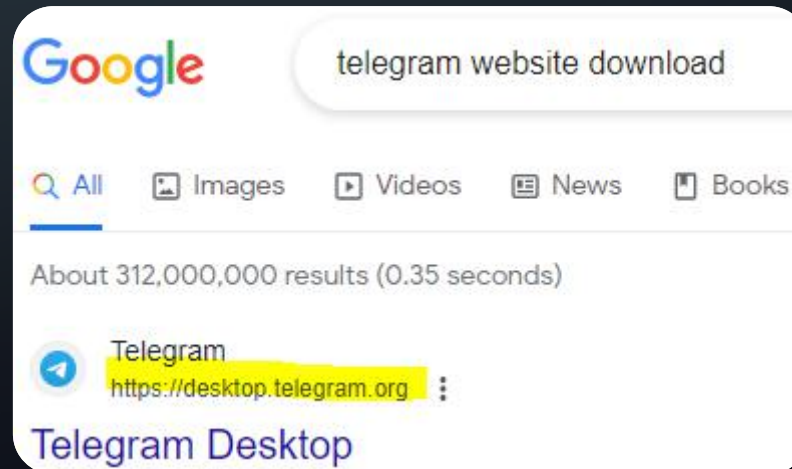


# Smart Phone Application Security



Only Install Applications which is coming from Known and Trusted Sources

**This is VITAL !**



paskoocheh.com

# Smart Phone Application Security



Check What  
Details Linked  
to Your Identity  
is Collected by  
the Applications



## Data Linked to You

The following data may be collected and linked to your identity:

- Health & Fitness
- Financial Info
- Contact Info
- User Content
- Browsing History
- Usage Data
- Diagnostics
- Purchases
- Location
- Contacts
- Search History
- Identifiers
- Sensitive Info
- Other Data

# Lockdown mode in iPhone

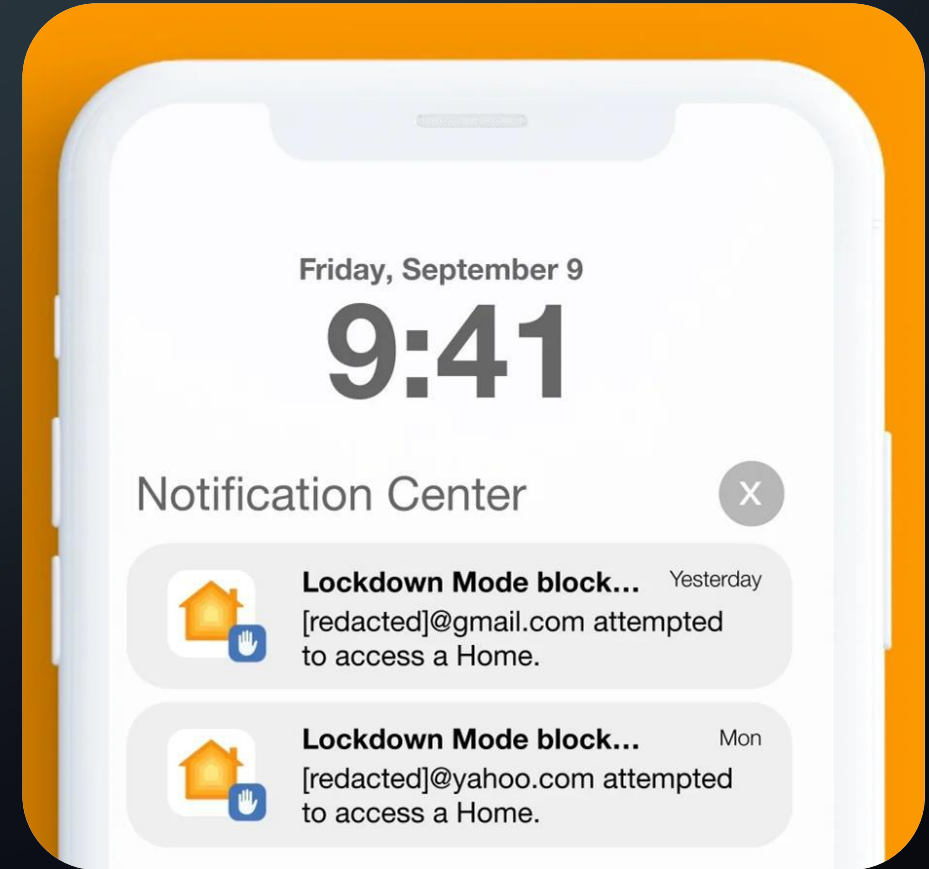
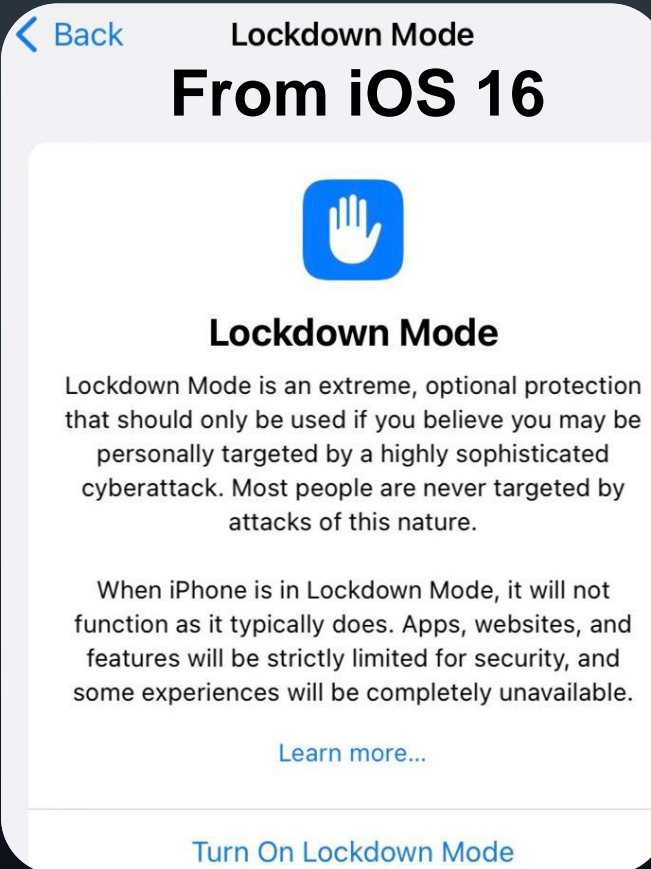


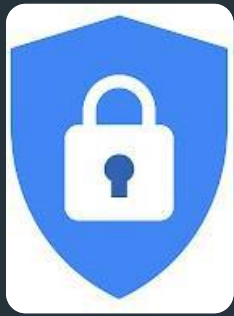
## Triple Threat

### NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains

By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, and Ron Deibert

April 18, 2023





# Google Advanced Protection Program (APP)

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

## 1. Two-Factor Authentication (2FA)

via Physical Security Key or Bluetooth Devices (no SMS or Authenticator)

## 2. Tightened Account Access

Limit Access to Google Services from non-Google Apps

## 3. Enhanced Email Protection

Advanced Phishing Detection and Warning & Blocking Unauthorized Access

## 4. Stronger Security Control

Restricts High-risk Activities, e.g., Download files or Grant access to 3<sup>rd</sup> party apps

## 5. Extra Protection Against Malware

Ability to use Google's Chrome browser in a more secure configuration

# # 1



تصور کنید یک دوست نزدیک و مورد اعتماد از شما درخواست می‌کند که برای ارسال امن یک فایل به شما نرم افزاری که با آن آشنایی قبلی ندارید رو در گوشی خود نصب کنید و لینک دانلود این نرم افزار رو از یک کانال تلگرامی برای شما دوست شما برای انتقال فایل توسط این میفرستد برنامه بشدت عجله دارد و امنیت وی ممکنه که در مخاطره باشه

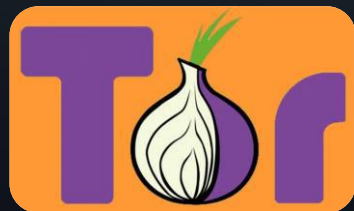
**در چنین موقعیتی چه کاری انجام می‌دهید؟**



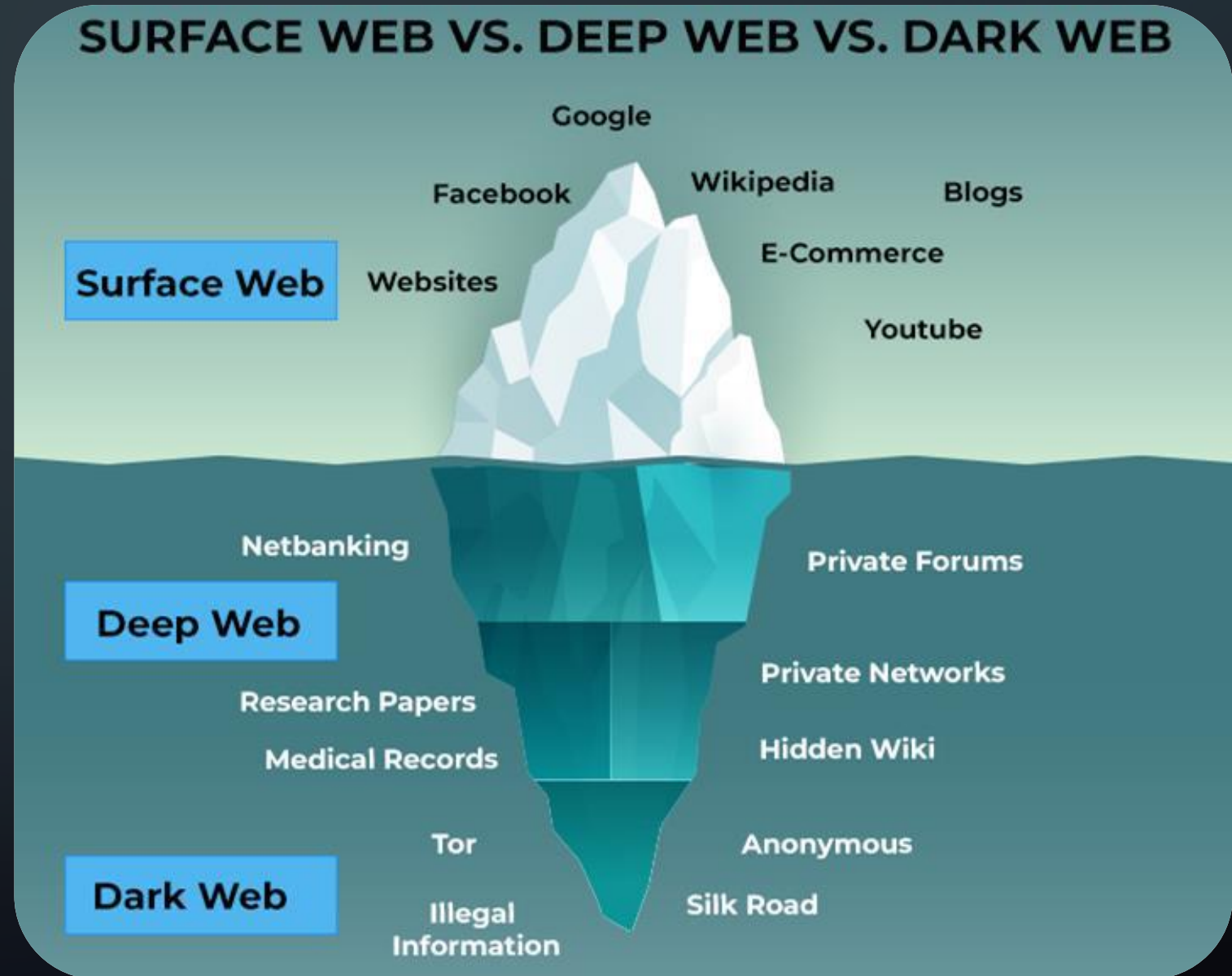
# Online/Web Security

How the REAL Internet looks like?

<https://www.torproject.org>



## SURFACE WEB VS. DEEP WEB VS. DARK WEB



# Online/Web Security

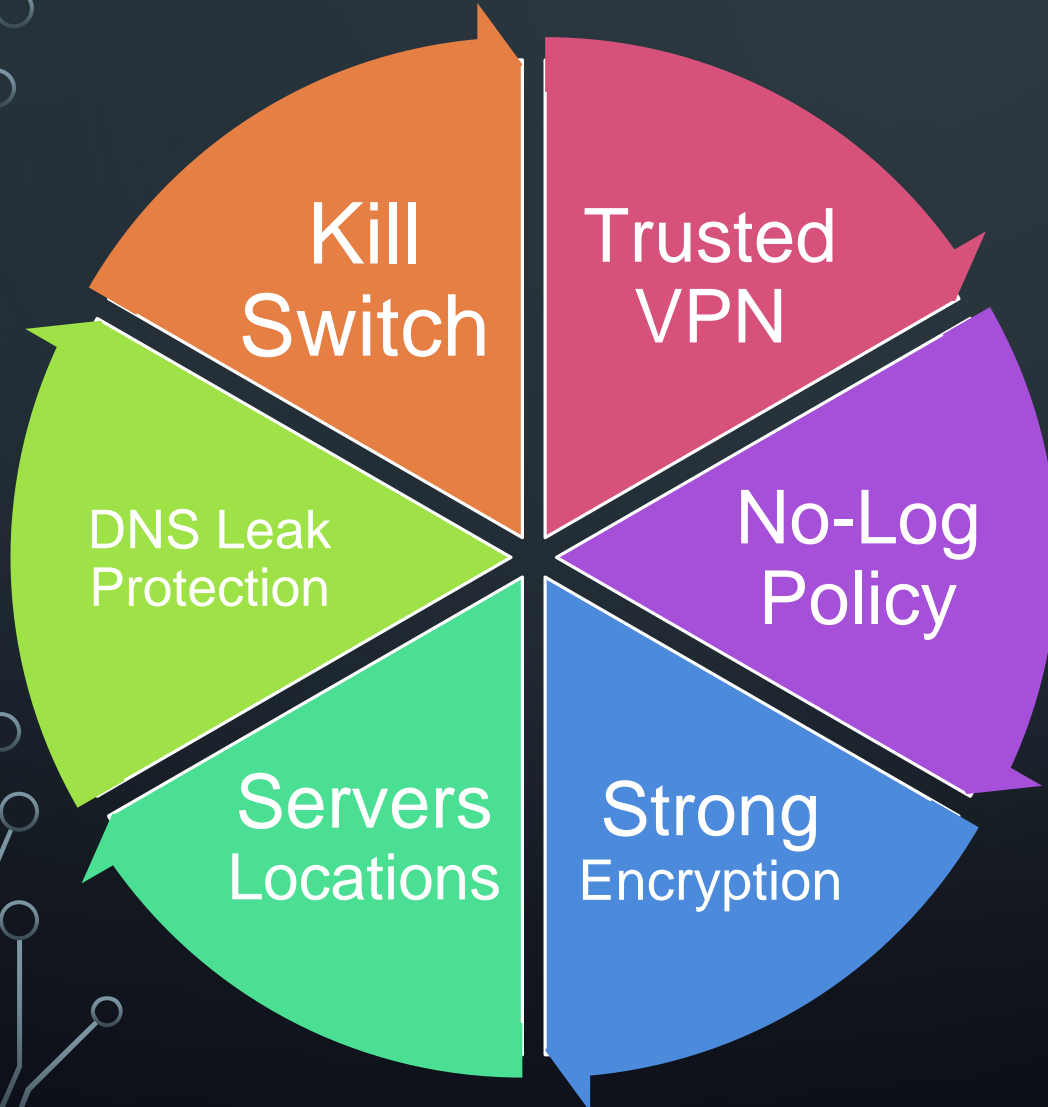
## 12 Key Points

to Minimize **Security**  
and **Privacy** Risks on  
the Internet



# Online/Web Security

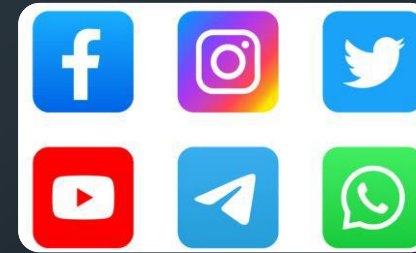
## Stay Anonymous



## Clean Footprint



**Emails**



**Social Media**



**Secure Browser**



**Private/Incognito browsing**

# Online/Web Security



**SECURELIST**

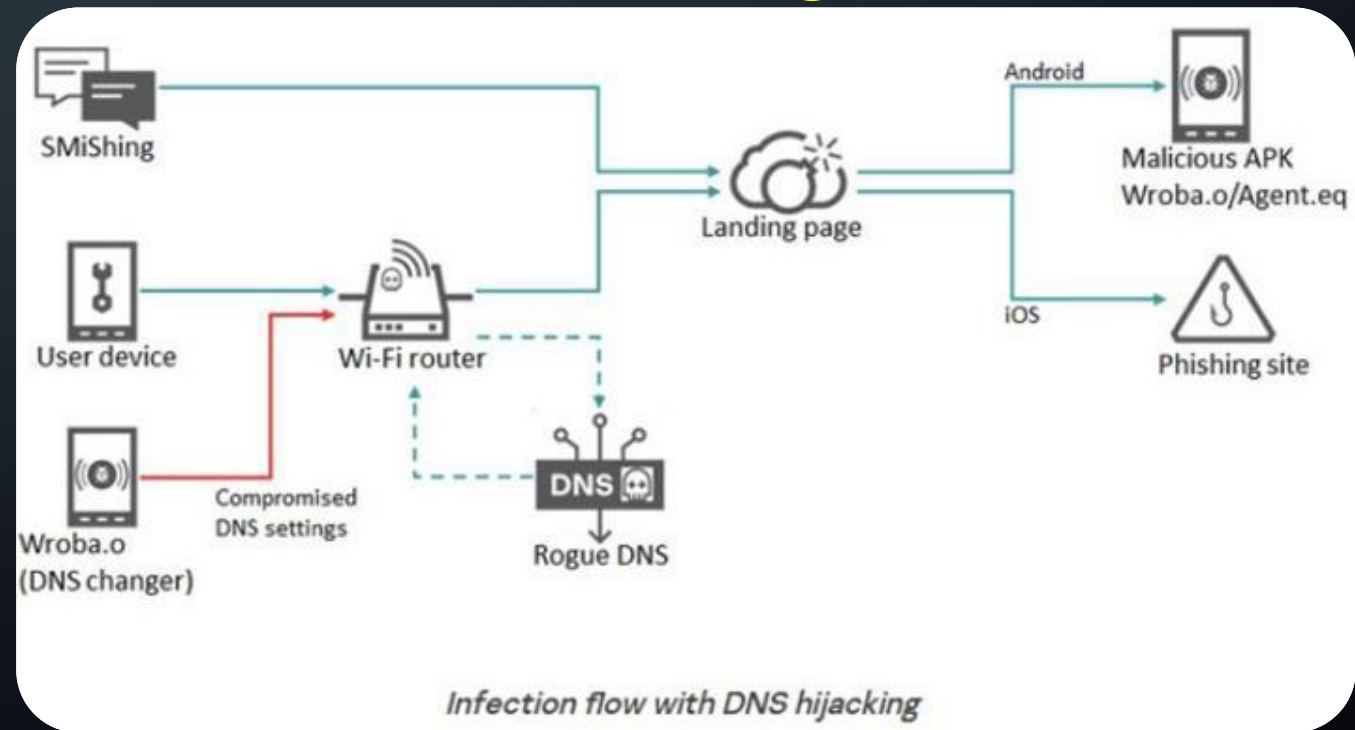
APT REPORTS

**Roaming Mantis implements new DNS changer in its malicious mobile app in 2022**

19 JAN 2023 6 minute read

Remember that If you've been hacked  
It is not JUST you.

Anyone in your Home/Office network  
can be affected and get hacked.



# # 2



همه شبکه های اجتماعی و تمامی وب سایتهای تجاری اقدام به گردآوری اطلاعات شخصی کاربران و دنبال کردن کاربران جهت ارسال در چنین تبلیغات هدفمند برای آنها میکنند شرایطی چه استراتژی و راهکاری میتوان بکار بست تا امنیت خود و اطرافیانمان در فضای مجازی رو ارتقا دهیم؟

**یک راهکار ساده و موثر در این خصوص پیشنهاد کنید.**

# Password Security



**Forbes**  
FORBES > INNOVATION > CYBERSECURITY  
EDITORS' PICK  
**New Dark Web Audit Reveals  
15 Billion Stolen Logins  
From 100,000 Breaches**


**Password cracking with NVIDIA RTX 4090**  
642 views · 15 hours ago SINGAPORE ...more

Too Many  
**Data Breaches**  
on Daily basis  
to Track



Personal Info  
and Passwords  
are on Sale on  
the **Dark Web**


# Password Security



300 billion hashes per second (GH/sec)  
200 thousand NTLM password hashes per second (kh/sec)

## Password cracking with NVIDIA RTX 4090

642 views · 15 hours ago SINGAPORE ...more

 Yaniv Hoffman 28.7K

Subscribe

Using Powerful Computers and GPUs, Hackers are able to **Crack the Password Hashes** and get your Plain Text Password.

# Password Security

<https://haveibeenpwned.com>

';--have i been pwned?

Check if your email or phone is in a data breach

email address

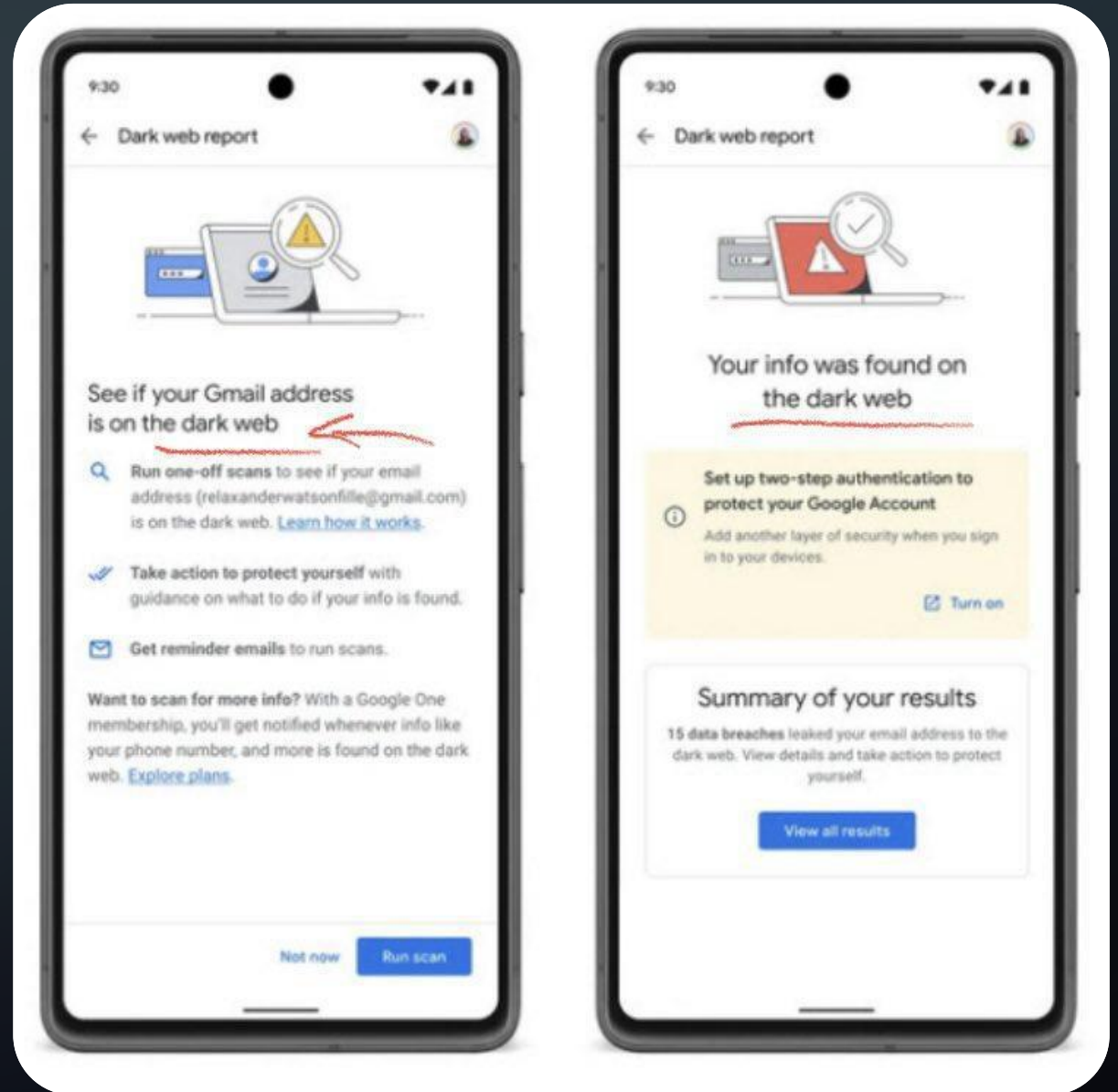
pwned?

a website that allows Internet users to check whether their personal data has been compromised by data breaches



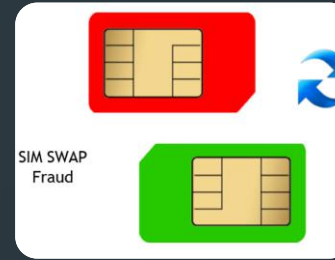
# Password Security

With a **Google One** membership, you can set up a profile to monitor the **Dark Web** so you can learn if your personal information is found in **Security Breaches**.

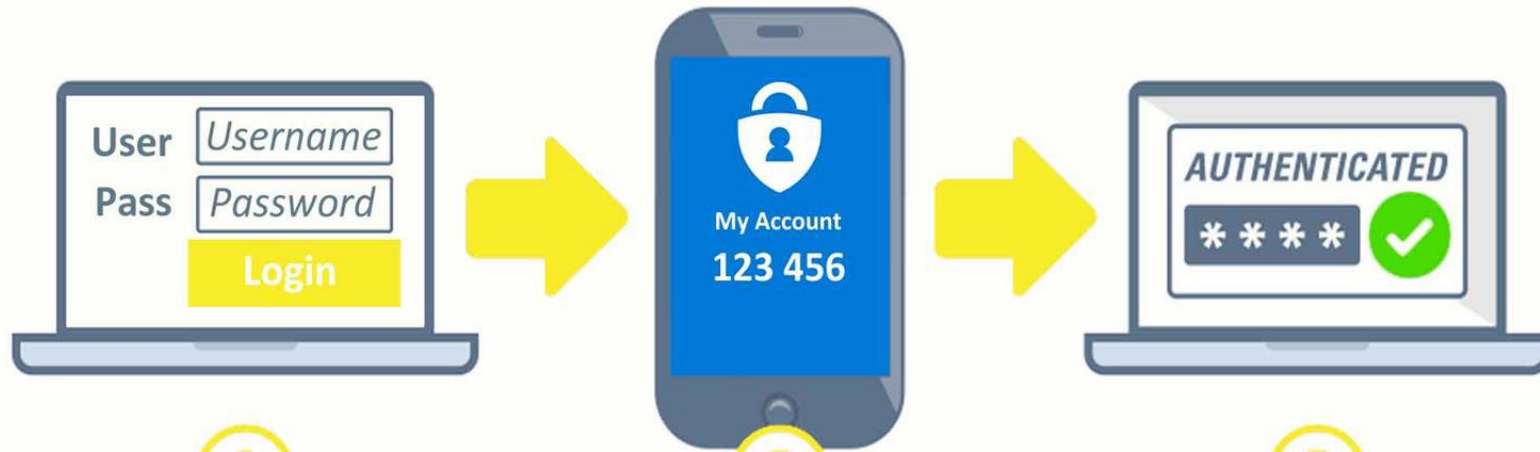
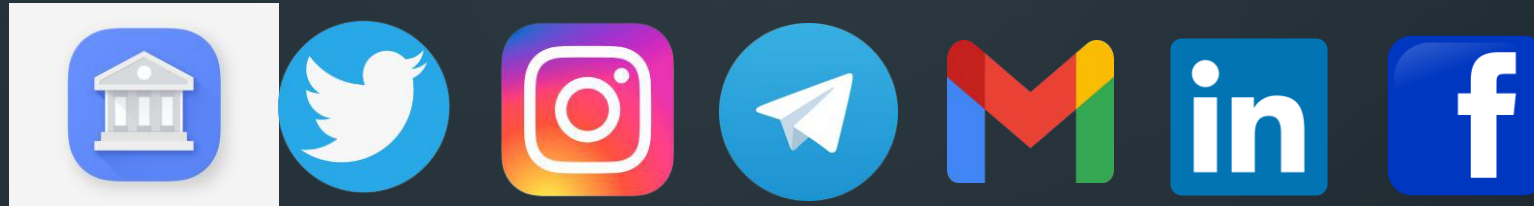


# 2-Factor Authentication (2FA)

Google Authenticator



SIM Card (Phone No.)



① User Logs in with Username & Password

② Authenticator App Generates (OTP) Code on Phone

③ User Enters the (OTP) Code and is granted access to the account.

access to the account

# Password Manager



1Password  
Bitwarden  
Dashlane



## 2FA and Passwordless Auth



# Password Sharing

Using Two Separate Channels (Email, Secure Chat, Phone)  
Or a **Password Manager**



# 3



استفاده از پسوردهایی که براساس الگو  
قفل گوشی رو باز میکنند علی رغم  
سهولت در استفاده از اونها ممکنه که  
امنیت گوشی شما رو به مخاطره بندازه .

استفاده از این نوع پسوردها چه ریسکهایی به همراه خواهد داشت ؟  
چطور میتوان ریسکهای احتمالی در این خصوص رو کاهش داد ؟

# App Privacy Report



## Android

1. Open "Settings" on your Android phone.
2. Scroll down & tap on "Apps & notifications."
3. Tap on "See all apps."
4. Select the app you want to check.
5. Tap on "Permissions."
6. Look for "Microphone" option and tap on it.
7. Here, you can see when the app last used microphone.

<https://www.instagram.com/reel/CsF8hNptcLX/?hl=en>



WhatsApp cannot be trusted



WhatsApp has been using the microphone in the background, while I was asleep and since I woke up at 6AM (and that's just a part of the timeline!) What's going on?

- 6:25 AM WhatsApp  
26 mins
- 5:59 AM WhatsApp  
2 mins
- 4:55 AM WhatsApp
- 4:41 AM WhatsApp  
14 mins
- 4:39 AM WhatsApp



Tweet your reply

# Recap

HTTPS/HSTS

Browsers

DNS Leak

Don't Use Public Wi-Fi Hotspots (MITM)

Cybersecurity Awareness

Trusted VPNs

Using AV and Ad Blocker

Updating Your Apps/System

Enable Disk Encryption

Avoid using End-of-Life & Out-dated Systems

Don't Visit Unknown Sites

Don't Click on Unknown Links

Don't Download Unknown Files

Thank You

Q & A

**1. Think Twice, CLICK Wise**

**2. Know Before INSTALL, Let's NOT Fall**

**3. NO PASSWORD Reuse, to STOP Abuse**

**4. Keep EVERYTHING Up-To-Date, to not become a BAIT**



<https://linktr.ee/5tuxnet>

