

# Digital & Device Security *in* Uncertain Times

Updated: 9 April 2025



# Table of Contents

1. Introduction to Security
2. Search and Seizure
3. On Spyware
4. Protecting Accounts from Hacking
5. Search Warrants and Warrantless Searches
6. Dealing with Doxxing and Harassment
7. Obfuscating Location
8. Secure Communication



# 1. Introduction to Security

# Two Useful Reminders

## 1. Daily Practice:

- Think of security as a daily shower, not a house repair project.
- Something you **practise daily** and not every few decades.

## 2. Keep Rehearsing:

- Under stress, sound decision making is affected.
- **Rehearsing** security notes is advised → easier to retrieve from memory under pressure.





# Working Towards Security

- **No silver bullet** exists for security, only **good daily practice**.
- Digital security **does not exist as a binary**  $\Rightarrow$  you can't qualify as either "safe" or "not safe."
- Your safety and security sits on a **spectrum**  $\Rightarrow$  the more you take safety measures the more you're protected against threats.
- It's about **risk and harm reduction**.



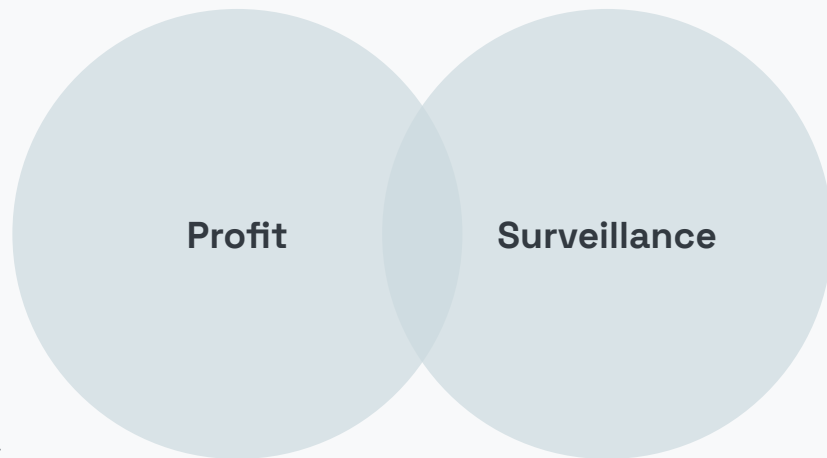
# Two Main Motives

Two main motives for breaching our security:

1. Profit
2. Surveillance

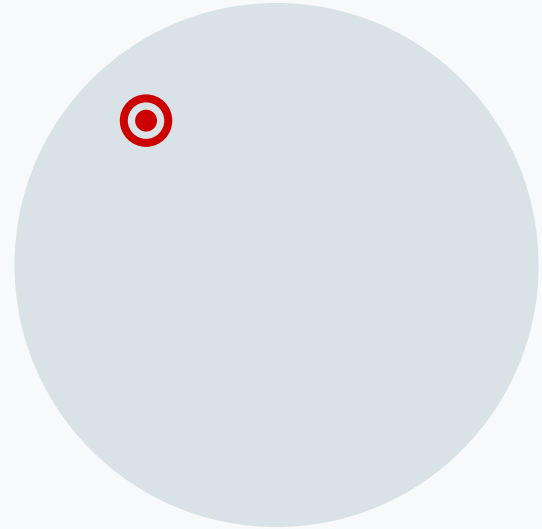
**Not mutually exclusive.**

*Perpetrators include companies, governments, intelligence agencies, individual hackers, organized crime groups, old friends or partners, etc.*



## Two broad types of threats:

1. **Untargeted** → motive is *usually* profit-making.
2. **Targeted** → motive is *usually* surveillance.



# Convenience vs. Security

# State Intelligence



# Civil Society

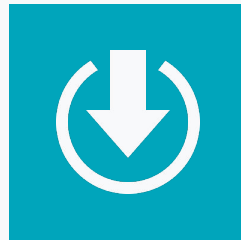
# Legend



**PREVENTATIVE**



**RESPONSIVE**



**TOOLBOX**

## 2. Search and Seizure

# Where Can Devices Be Seized?

- Borders or checkpoints
- Protests
- Conflict sites
- During a house or office raid



IMAGE SOURCE: EFF.ORG



# What Can Police Do?

Depending on your location and context, police may take different approaches. While most law enforcement agencies worldwide have digital forensic capabilities, some simply conduct a quick manual search of a device, such as what typically happens at checkpoints.

## Manual Search

- Police take the device.
- Ask you to unlock it.
- Device is searched for "incriminating" content.
- Often conducted in **front of you**.
- Device usually **remains in your sight**.

vs.

## Digital Forensic Search

- Police take the device.
- Device is transported to **another location**.
- Device is connected to **specialized equipment**.
- Device data is **fully extracted**.
- Process can take **months**, device might not return.

# On Digital Forensic Search

Police worldwide use forensic tools such as **Cellebrite** and **Graykey** to:

1. **Crack** through locked devices.
2. **Extract** all of the device's data.

These tools can extract: messages, files, photos, passwords, login sessions, deleted data (not all), and much more.





Cellebrite Touch

TOUCH

Select Extraction Type



Logical Extraction



Password Extraction



SIM Data Extraction



Clone SIM



File System Extraction



Physical Extraction



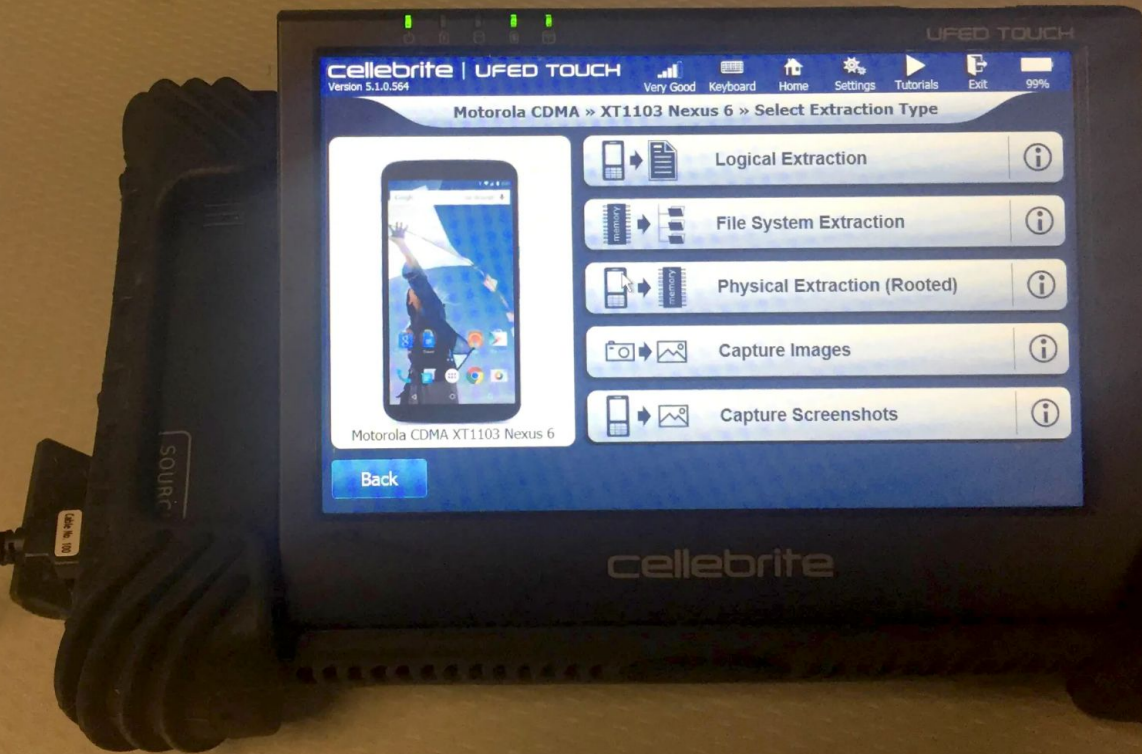
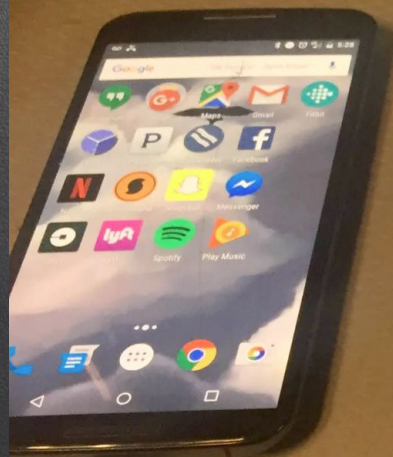
Device Tools

cellebrite

SOURCE

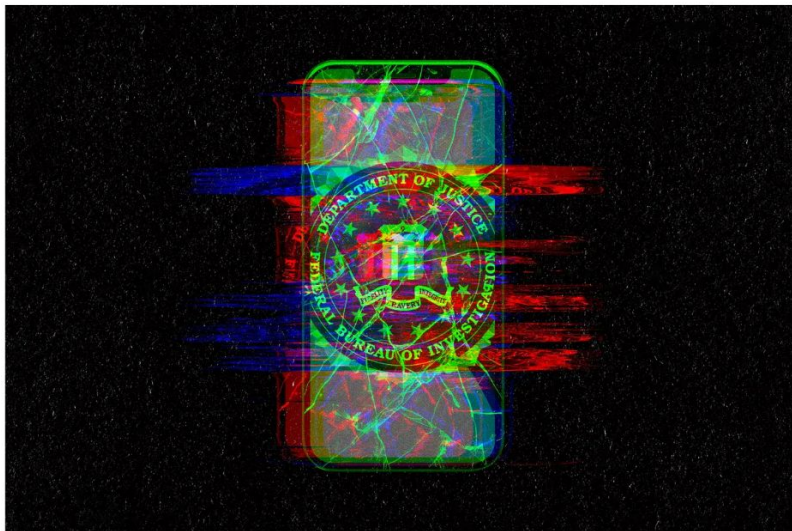
TARGET





POLICY / US &amp; WORLD / TECH

# The FBI got into the Trump rally shooter's phone in just 40 minutes



/ The bureau reportedly used an unreleased Cellebrite tool to open the phone.

By [Gaby Del Valle](#), a policy reporter. Her past work has focused on immigration politics, border surveillance technologies, and the rise of the New Right.

Jul 19, 2024, 6:53 PM GMT+3

# Can Police Crack All Phones?

We cannot be sure, but we know that police have a **tougher time** to crack a phone's lock using tools like Cellebrite if:

- 📱 Your phone's **operating system** is up-to-date.
- ⚙️ Your phone uses **modern hardware** (i.e. has a modern chip).
- 🔒 Your phone is **locked** with a strong and complex passcode.
- 🔄 The phone was **shut down** when it was seized, or **just restarted** and never unlocked since last restart.\*

⚙️ For iPhones: if you have **Lockdown Mode** enabled.

*\* Files on the device are better secured if the phone was just restarted and hasn't been unlocked yet.*



Table 1: iPhones Support Matrix 7.69.1 Locked

Newly added

iPhone	SoC	≤11	12.0-12.5.x	13.1-13.7.x	14.0-14.8.x	15-15.8.x	16.0-16.7.x	17.0 - 17.0.3	17.1-17.3.1	17.4 - Newer
iPhone 5   iPhone 5C   iPhone 5S   iPhone 6   iPhone 6+	A6  A7  A8	BF	BF	N/A	N/A	N/A	N/A	N/A	N/A	N/A
iPhone 6S   iPhone 6S+   iPhone SE gen 1   iPhone 7   iPhone 7+	A9   A10	BF	Supersonic BF	Supersonic BF	Supersonic BF	Supersonic BF	N/A	N/A	N/A	N/A
iPhone 8   iPhone 8+   iPhone X	A11	BF	Supersonic BF	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)(6)	N/A	N/A	N/A
iPhone XR   iPhone XS max   iPhone XS	A12	N/A	BF	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)	AFU + IPR + Supersonic B F (1)(4)	Supersonic BF (1)(4)	In Research
iPhone 11   iPhone 11 pro   iPhone 11 pro max   iPhone SE gen 2	A13	N/A	N/A	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)	AFU + IPR + Supersonic B F (1)(4)	Supersonic BF (1)(4)	In Research
iPhone 12   iPhone 12 pro   iPhone 12 pro max  iPhone 12 mini	A14	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 13   iPhone 13 pro   iPhone 13 pro max   iPhone 13 mini   iPhone SE gen 3	A15	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 14   iPhone 14 Plus   iPhone 14 pro   iPhone 14 pro max	A16   A15	N/A	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 15   iPhone 15 Pro   iPhone Pro Max	A16  A17	N/A	N/A	N/A	N/A	N/A	N/A	In Research	In Research	In Research

# Table 2: Android OS Access Support Matrix – Locked devices 7.69.1

Vendor (Chipset)		Section 1: COLD - turned off (Secure startup or FBE)		Section 2: HOT (AFU or FDE without secure startup)		Comments and exceptions	
		BFU extractions (for FBE devices)	Brute-Force Password to get the user data (CE) decrypted	All Extractions (Even without BF)	Brute-Force password (not needed for extraction)		
Samsung (Exynos / MTK / Qualcomm)	Android 6	✗	✗	✓	✓		<div>  Fully Supported         </div> <div>  Partially Supported         </div> <div>  Not Supported         </div>
	Android 7-14	✓	✓	✓	✓	Added BF support for QC S24, S24+, S24 Ultra	
Huawei (Kirin / Qualcomm / MTK)		✓	✓	✓	✓	P40 family is supported for Brute-force only up to ~04-2021 SPL	
Pixel	Pixel, Pixel XL	✓	✓	✓	✓		<div>  Huawei Kirin temporarily disabled.         </div>
	Pixel 3 - 5	✓	✓	✓	✓	Added AFU support for Android 14 Official and Pixel 8.	
	Pixel 6 - 8	✓	✗	✓	✗	BF support for Pixel 3-5 extended to latest SPLs	
Non-Samsung Qualcomm including Huawei, LG, Motorola, Xiaomi, Sony, OnePlus and many more		✓	✓	✓	✓	Added AFU, BFU & BF support for Snapdragon 8 Gen 3, 8 Gen 2, 6 Gen 1, 7+ Gen 2, 7s Gen 2, 4 Gen 2.	<div>  For Non-Samsung/Pixel, Qualcomm FBE devices, there may be a requirement for 24hr uptime of the device prior attempting to brute force the device. Affected chipsets: SM4350, SM6150 SM7150, SM8150 and newer.         </div>





# Preventative Tips



- Set a strong **passcode** for your device.
- Turn off **biometric lock**.
- Update device **operating system**.
- Turn off **control panel** from lock screen.
- Lock your **SIM card** (add a pin code).
- Enable **Lockdown Mode** (iPhones only).
- **Delete sensitive data** from device.
- Ensure you can **locate** your device remotely (check next slides).

- **Hide apps** from home screen if possible.
- Change **app icons** where possible.
- Enable **disappearing messages**.
- Place files, media in secure folders ([Tella](#)).
- Hide notification content from lock screen.

[Click here for a more detailed guide.](#)

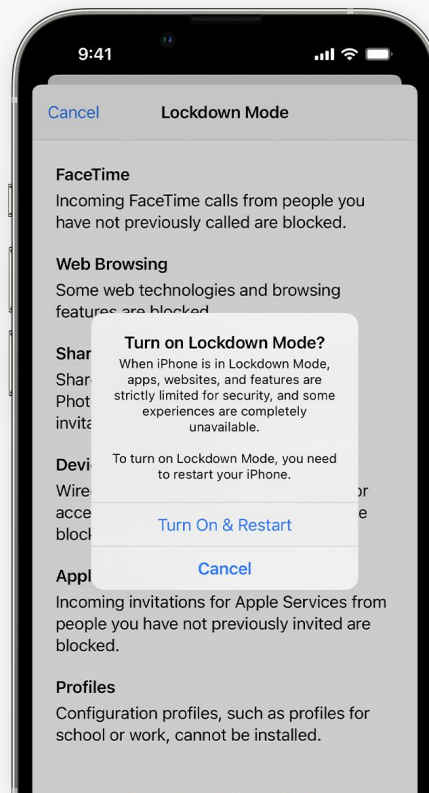


# Lockdown Mode on iPhone



- Apple released a feature called Lockdown Mode to protect highly at-risk users against **sophisticated cyber attacks**.
- To activate it, go to: **Settings > Privacy & Security > Lockdown Mode**.

*To date, researchers have not found a single iPhone that was successfully infected with spyware or had its lock successfully broken when Lockdown Mode was activated.*



# Responsive Tips



→ Keep the device **locked** and **resist** handing over the passcode (during seizure).

## After seizure:

→ Locate and **remotely wipe** device data.

→ **Change passwords** for all accounts on device.

→ Request platforms to **disable** accounts.



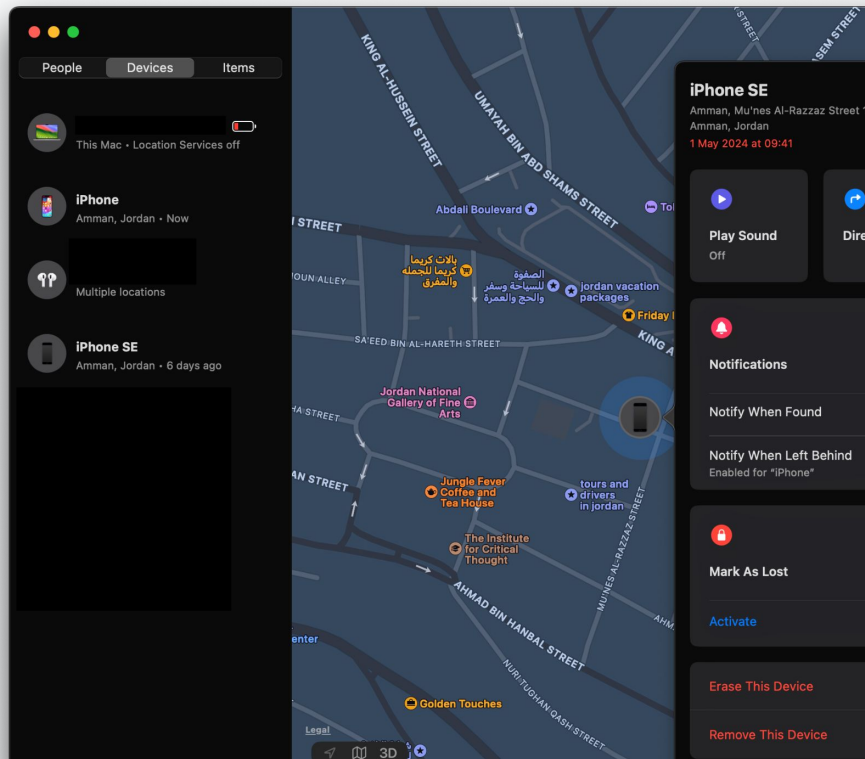
# Remotely Wiping Devices



Following seizure, you may still have the option to **locate your device** online and remotely initiate a full content deletion (action cannot be reversed):

- For Android: [android.com/find](https://android.com/find)
- For iOS: [icloud.com/find](https://icloud.com/find)

**Note:** Your device must be online for this to work.  
Police often put phones in airplane mode!



# 3.

## On Spyware

# What is Spyware?

- Spyware is malicious software that **installs itself** on a device – without the target's knowledge or consent – to **spy on the target**.
- Spyware can:
  - See virtually **everything stored on the device** (messages, files, photos, passwords, browsing history),
  - **Conduct live surveillance** (through microphone and camera),
  - **Transmit this data to the surveilling party** (often a state).



NSO GROUP

20/05/2012 16:14

Welcome Gilgi Admin | Sign out

Back to Previous

Look for: All Int: All

Groups

- burning
- iPhone
- Android
- Sony ericson
- 991
- hello~I install me
- play1
- play2
- nex
- 42 44
- recordingh
- record

Dashboard

Map (2)

Rules & Alerts

Call Log (27)

Direction	Duration	Timestamp	Recorded
Outbound	00:00:15	5/20/2012 3:55:00 PM	
Outbound	00:00:44	5/20/2012 3:53:15 PM	
Outbound	00:00:00	5/20/2012 3:44:36 PM	
Outbound	00:00:00	5/20/2012 2:01:00 PM	
Outbound	00:00:00	5/20/2012 1:52:41 PM	
Outbound	00:00:00	5/20/2012 1:50:35 PM	
Outbound	00:00:11	5/14/2012 5:10:04 PM	
Inbound	00:00:00	5/14/2012 4:32:18 PM	
Outbound	00:00:05	5/10/2012 2:01:37 PM	
Outbound	00:00:04	5/10/2012 12:26:09 PM	
Outbound	00:00:10	5/10/2012 12:25:36 PM	
Outbound	00:00:57	5/10/2012 12:05:57 PM	
Outbound	00:00:00	5/9/2012 3:12:49 PM	
Inbound	00:00:00	5/9/2012 8:12:52 AM	
Inbound	00:00:00	5/8/2012 7:51:23 PM	
Outbound	00:17:06	5/7/2012 1:37:43 PM	
Outbound	00:09:57	5/7/2012 1:25:07 PM	
Outbound	00:05:11	5/7/2012 11:36:20 AM	
Outbound	00:00:00	5/7/2012 11:36:06 AM	
Outbound	00:00:00	5/1/2012 7:14:49 PM	
Inbound	00:00:01	5/1/2012 4:46:12 PM	
Outbound	00:00:06	5/1/2012 1:02:18 PM	
Outbound	00:00:06	5/1/2012 11:33:47 AM	

Export

Call Recording Configuration

Call Recording is: ☒ Enabled

Disable

Sent Timestamp: 5/20/2012 12:53:05 PM

Received acknowledge: 5/20/2012 12:53:14 PM

Playback

00:07 / 00:28

Description:

0

Save Edit

Close





NSO GROUP

Android > Agent record Number: 9999999999 IMEI:

Groups

burning

iPhone

Android

Sony ericson

991

hello~I install me

play1

play2

nex

42 44

recordingh

record

Dashboard

Map (2)

Rules & Alerts

Export

20/05/2012

★

📍

📁

✉

@

💬

☎

📅

🎤

📷

📁

⌚

💻

📄

✂

⚙

ℹ

Favorites (0)

Location (68)

Contacts (360)

Messages (70)

Email (50)

IM (7)

Call Log (31)

Calendar (4)

Tap (2)

Camera S... (6)

Dir List (20)

Misc (7)

Commands (29)

Log (32)

Configur... (1)

Installati... (1)

Device Info

2011

2012

2013

Chats

★	Type	Timestamp	Participants
★	📞	10/6/2013 1:14:47 PM	Mr. John Doe( )
★	📞	10/6/2013 1:02:22 PM	Mr. John Doe( )
★	📞	9/16/2013 8:01:32 PM	Mr. John Doe( )
★	📞	9/16/2013 10:35:33 AM	Mr. John Doe( )
★	📘	9/14/2013 2:51:07 PM	
★	📘	9/11/2013 8:49:35 PM	
★	📘	9/9/2013 12:59:34 PM	

Details

Conversation:

7/29/2013 2:52:46 PM:  
Mr. John Doe:What's up

7/29/2013 2:52:55 PM:  
Mr. John Doe:Are you coming?

7/29/2013 2:53:08 PM:  
:Yes

7/29/2013 2:53:29 PM:  
:When do you want us to meet?

7/29/2013 2:53:36 PM:  
:And where

7/29/2013 2:54:06 PM:  
Mr. John Doe:Come to the down town square

7/29/2013 2:54:11 PM:  
Mr. John Doe:At 20:00

7/29/2013 2:54:20 PM:  
Mr. John Doe:Don't be late!!

7/29/2013 2:54:30 PM:  
:Ok see you there

8/12/2013 5:57:23 PM:  
Mr. John Doe:Are you there

9/16/2013 9:35:33 AM:  
Mr. John Doe:Hello my friend





# Spyware Landscape

- The spyware landscape is **wide**.
- A multitude of commercial vendors.
- Infamous names:
  - **Pegasus** by NSO Group.
  - **Predator** by Intellexa Consortium.
  - **Graphite** by Paragon.

Name	Aliases	Spyware products	0-days targeting Google products		0-days targeting other products	
Candiru	remora-tech	DevilTongue	CVE-2021-2166	Google Chrome	CVE-2018-5002	Adobe Flash [1, 2]
	candiru		CVE-2021-30551	Google Chrome	CVE-2021-31979	Microsoft Windows
	cyna-tech		CVE-2022-2294	Google Chrome	CVE-2021-33742	Microsoft Internet Explorer
	nerfwall		CVE-2022-3723	Google Chrome	CVE-2021-33771	Microsoft Windows
	tavetasolution		CVE-2023-5217	Google Chrome		
Cy4Gate		Epeius	CVE-2021-22600	Linux kernel, exploited against Android		
			CVE-2021-25394	Samsung MFC charger driver, exploited against Android		
			CVE-2023-4211	Arm Mali GPU, exploited against Android		
			CVE-2023-33106	Qualcomm Adreno GPU, exploited against Android		
			CVE-2023-33107	Qualcomm Adreno GPU, exploited against Android		
DSIRF		Subzero			CVE-2021-28550	Adobe Reader
					CVE-2021-31199	Microsoft Windows
					CVE-2021-31201	Microsoft Windows
					CVE-2021-36948	Microsoft Windows
					CVE-2022-22047	Microsoft Windows
Intellexa	Cyrox	Nova	CVE-2019-2215	Android kernel	CVE-2023-41991	Apple iOS
	Nesa Technologies	Triton	CVE-2021-1048	Google Android	CVE-2023-41992	Apple iOS
	Wispear	Helios	CVE-2021-1905	Qualcomm Adreno GPU, exploited against Android	CVE-2023-41993	Apple iOS
		ALIEN (stager)	CVE-2021-1906	Qualcomm chipsets, exploited against Android		
		PREDATOR (Android/iOS)	CVE-2021-28644	Arm Mali GPU, exploited against Android		
			CVE-2021-39793	Arm Mali GPU, exploited against Android		
			CVE-2021-30554	Google Chrome		
			CVE-2021-37973	Google Chrome		
			CVE-2021-37976	Google Chrome		
			CVE-2021-38000	Google Chrome		
			CVE-2021-38003	Google Chrome		
			CVE-2022-3075	Google Chrome		
			CVE-2023-2033	Google Chrome		
			CVE-2023-2136	Google Chrome		
			CVE-2023-3079	Google Chrome		
			CVE-2021-28663	Arm Mali GPU, exploited against Android	CVE-2022-42856	Apple Safari
			CVE-2022-3723	Google Chrome		
			CVE-2022-4135	Google Chrome		
NSO Group	Q-Cyber	PEGASUS ( Android/ iOS)	CVE-2019-2215	Android kernel	CVE-2016-4655	Apple iOS
	Circles		CVE-2023-7024	Google Chrome	CVE-2016-4656	Apple iOS
					CVE-2016-4657	Apple iOS
					CVE-2019-3568	Facebook WhatsApp
					CVE-2021-30860	Apple iOS
					CVE-2021-31010	Apple iOS
					CVE-2023-41061	Apple iOS
					CVE-2023-41064	Apple iOS
					Exploits without publicly confirmed CVE's: KISMET, exploited against Apple iOS	
PARS Defense					CVE-2023-42916	Apple WebKit
					CVE-2023-42917	Apple WebKit
QuaDream					Exploits without publicly confirmed CVE's: ENDOFDAYS, exploited against Apple iOS	
RCS Lab					CVE-2021-30883	Apple iOS kernel
					CVE-2021-30983	Apple iOS kernel
Variston	Variston IT	Heliconia	CVE-2022-4262	Google Chrome	CVE-2022-26485	Mozilla Firefox
	TrueIT	(exploitation framework)	CVE-2023-0266	Google Android	CVE-2023-28205	Apple WebKit
	Protected AE	BridgeHead	CVE-2023-21492	Samsung Android	CVE-2023-28206	Apple iOS
			CVE-2023-26083	Arm Mali GPU, exploited against Android	CVE-2023-32409	Apple WebKit
	EdgeGroup		CVE-2023-33063	Qualcomm Adreno GPU, exploited against Android		
Wintego Systems			CVE-2019-2215	Android kernel		
			CVE-2021-0920	Google Android		
			CVE-2022-2856	Google Chrome		

# How Are Devices Hacked?



A **link** that you're tricked into clicking.



A **file** that you're made to download and open.



Malicious **USBs** inserted into your device.



Malicious **websites**.



Through an **unsecured Wi-Fi** network.



Reckless **device use**, such as leaving it open and unattended.




No action from your side → **zero-click attacks**.

# How Are Devices **Commonly** Hacked?


 A **link** that you're tricked into clicking.

 A **file** that you're made to download and open.

 Malicious **USBs** inserted into your device.

 Malicious **websites**.

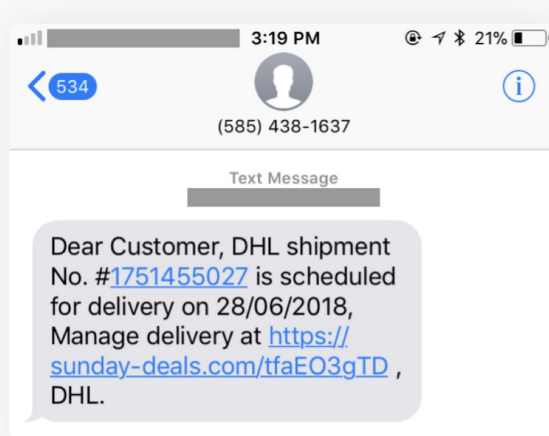
 Through an **unsecured Wi-Fi** network.

 Reckless **device use**, such as leaving it open and unattended.

 No action from your side → **zero-click attacks**.

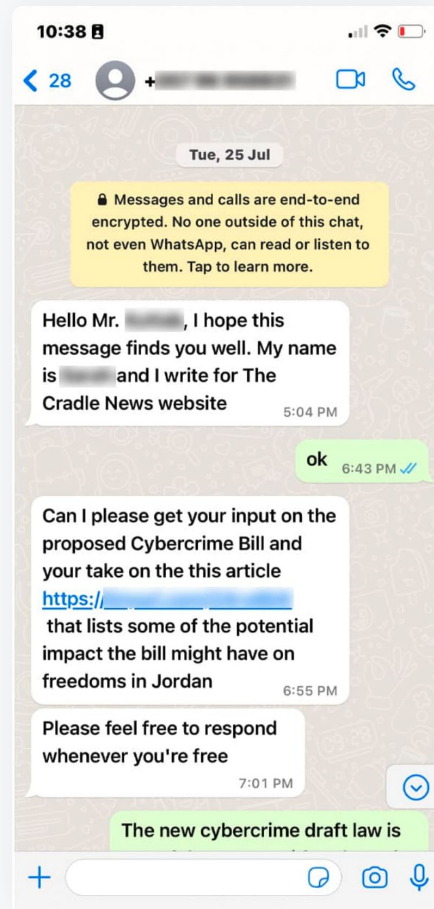
# Saudi Dissident in Exile

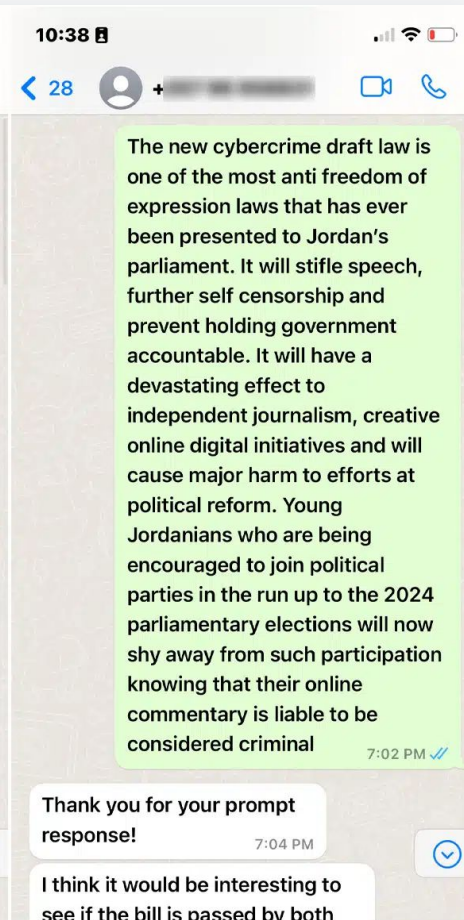
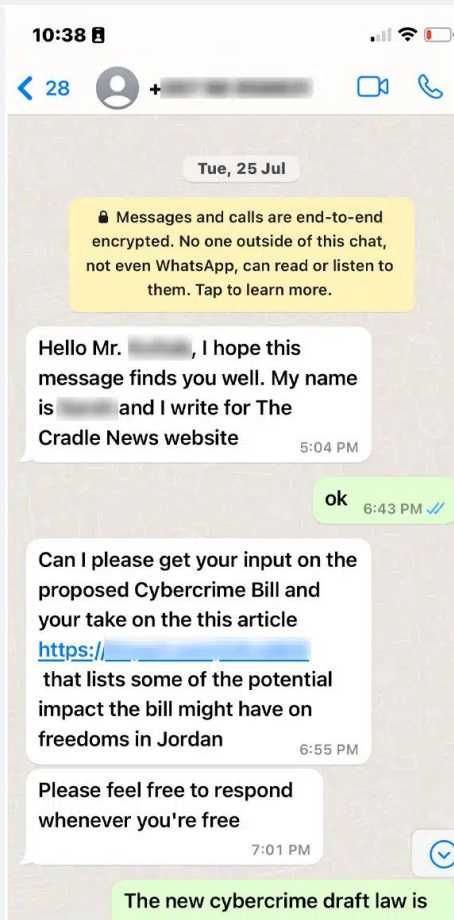
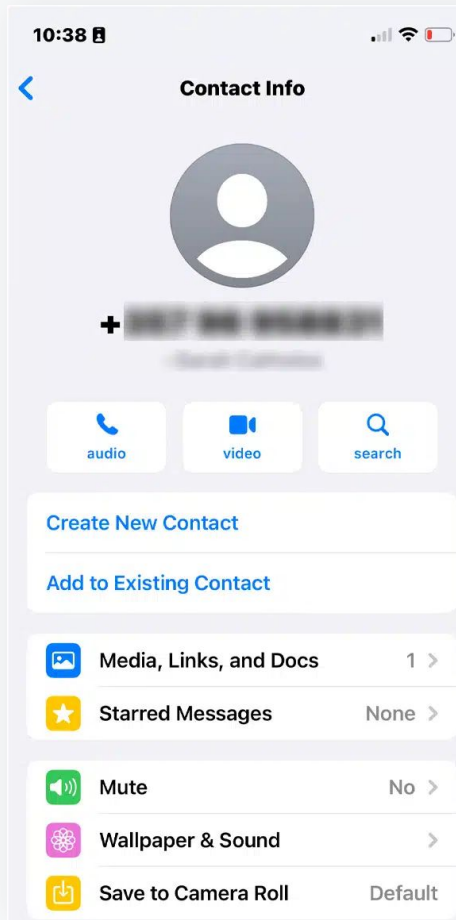
- Omar Abdulaziz, friend of Jamal Khashoggi, Saudi political activist **living in exile** in Canada.
- One day in 2018, Abdulaziz made a purchase on Amazon. Later that day he received an SMS purporting be a package shipment notification from DHL.
- The URL in the message was from the domain **sunday-deals[.]com**, which The Citizen Lab identified as a **Pegasus domain** (i.e. clicking on the link would result in Abdulaziz's phone infection).

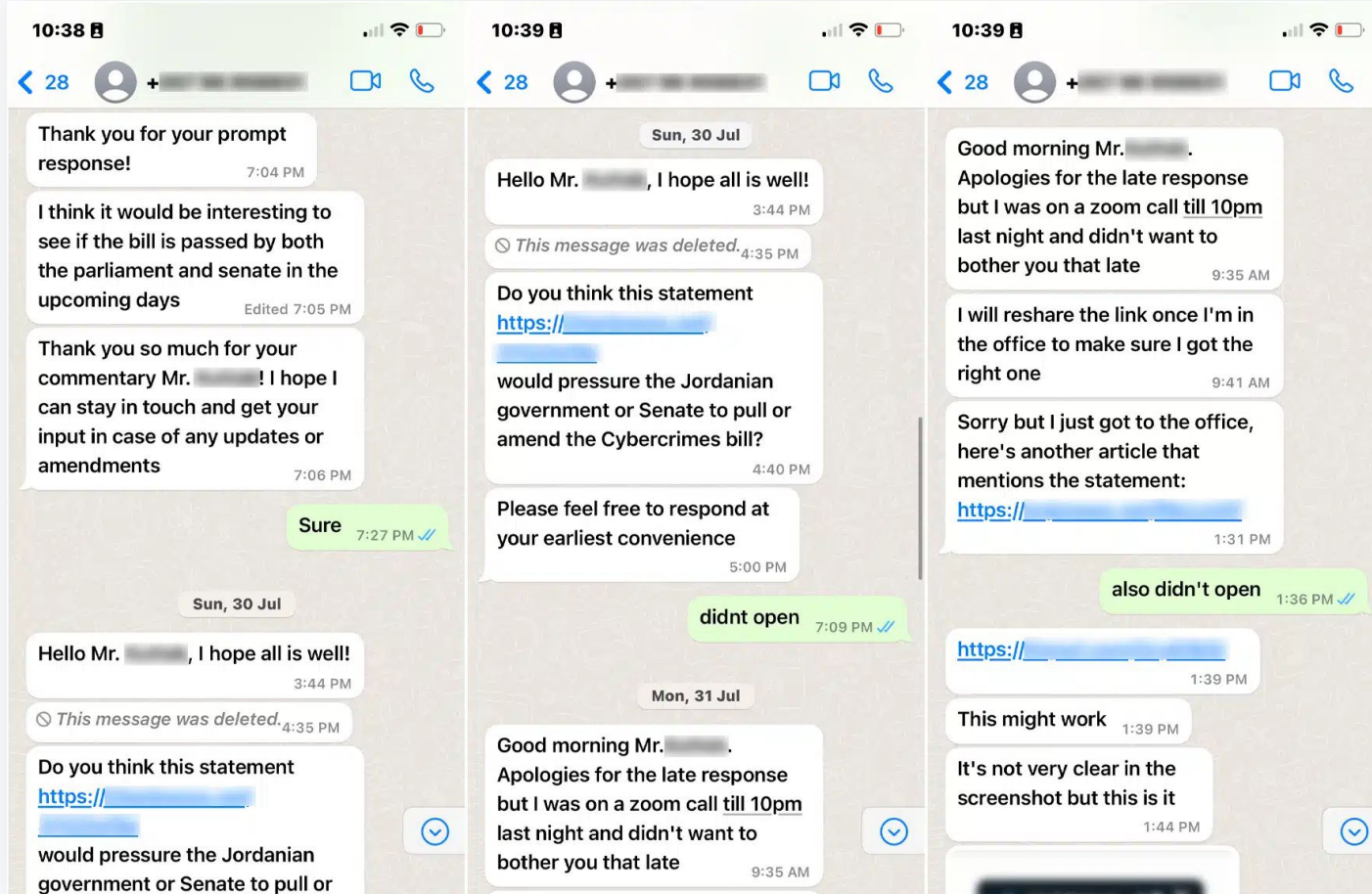


# Pegasus'd via WhatsApp

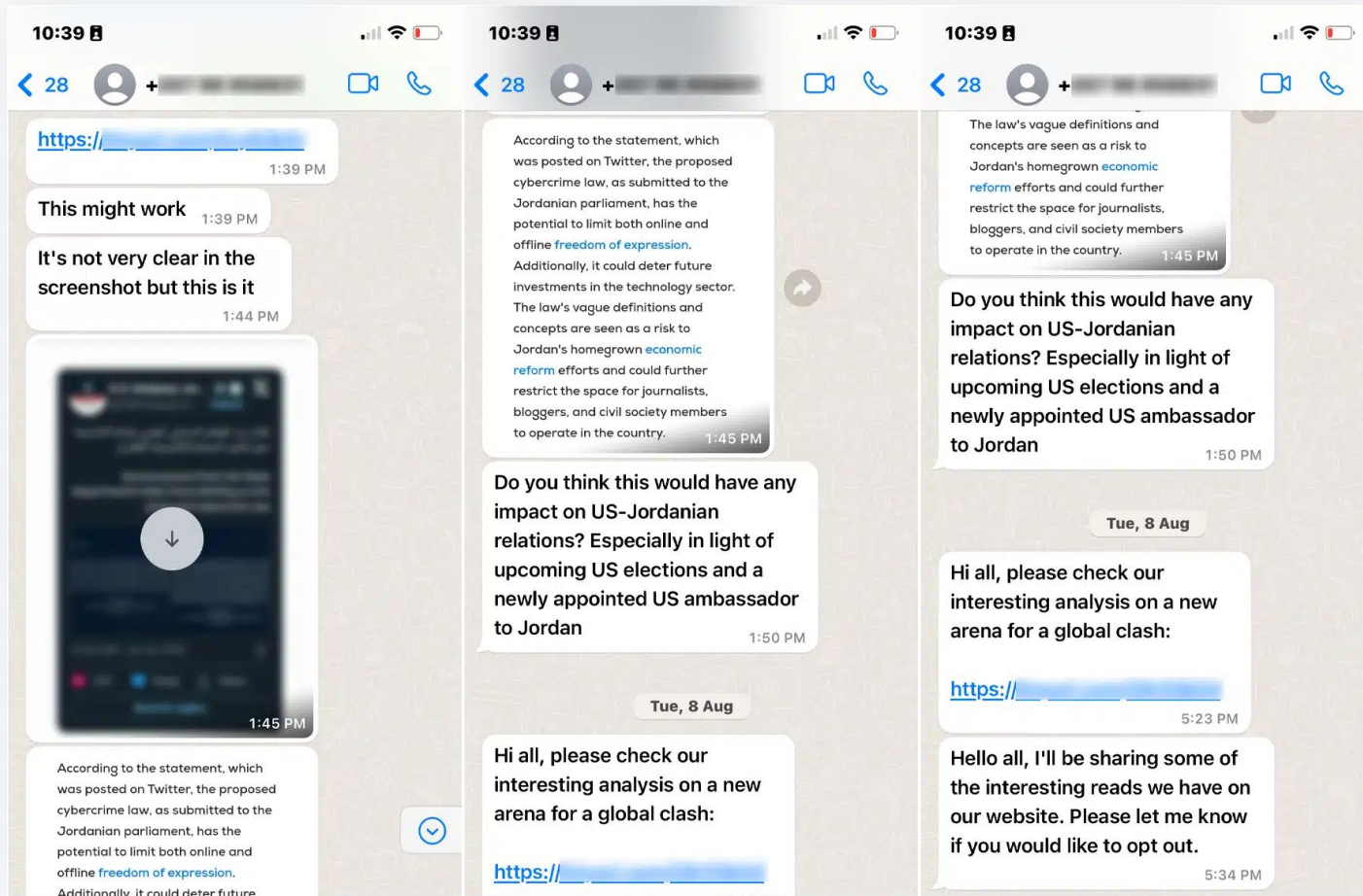
- Daoud Kuttab is a Palestinian-American journalist based in Jordan.
- In the summer of 2023, Kuttab received a message on WhatsApp from someone **claiming to be a journalist** from The Cradle and asking for Kuttab's input on a local draft law.
- The message contained URLs that The Citizen Lab identified as **Pegasus domains**.
- Kuttab was found to be hacked **multiple times** between February 2022 and September 2023.















Joseph Gordon @Joseph\_Gordon16

[caavn.org/news/china/article...](https://caavn.org/news/china/article...)

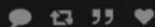
Apr 14



### US defence contractors visiting Taiwan in May to boost se

Two dozen industry representatives, led by retired US Marine Corps, expected to discuss drone technology among other issues.

[scmp.com](https://scmp.com)



Thoibao.de @thoibao\_de · Feb 4

Serious incidents in Vietnam's Defense Ministry: Corrupted generals face prosecution



thoibao.de

Serious incidents in Vietnam's Defense Ministry: ...  
Vietnam's Ministry of Defense is considered a place of dispute between the General Secretary o...



1



5



842



Joseph Gordon

@Joseph\_Gordon16

Cong an dau da noi bo, Bo Cong an bat cong an Hai Duong  
[Inktonews.co/MEmk](https://Inktonews.co/MEmk)

8:19 AM · Feb 9, 2023 · 12 Views



**Joseph Gordon** @Joseph\_Gordon16 · Apr 14  
[caavn.org/news/china/article...](https://caavn.org/news/china/article...)



**South China Morning Post**

**US defence contractors visiting**  
 Two dozen industry representatives, expected to discuss drone technology  
[scmp.com](https://scmp.com)

**Mission Ocean Waters** @eumissionocean · 21h

"We have decided to transform how we live on Aran Islands with a population of 1500 on three islands.

"Individually Inis Mór (large island) has a population of 1000 people, Inis Meáin (middle island) has 200 inhabitants and Inis Oírr (easterly Island) although the smallest... [Show more](#)



7 23 110 11.9K

**Joseph Gordon** @Joseph\_Gordon16 · 8h  
 Replying to @eumissionocean  
 As more nations oppose China, how seriously does the world take Beijing? [southchinapost.net/VuAfn](https://southchinapost.net/VuAfn)

32

4

**Defense Ministry: Corrupted generals face**

2

idents in Vietnam's Defense Ministry: ...  
 Ministry of Defense is considered a  
 dispute between the General Secretary o...

5 842

... bat cong an Hai Duong

# What About Zero-Click Attacks?

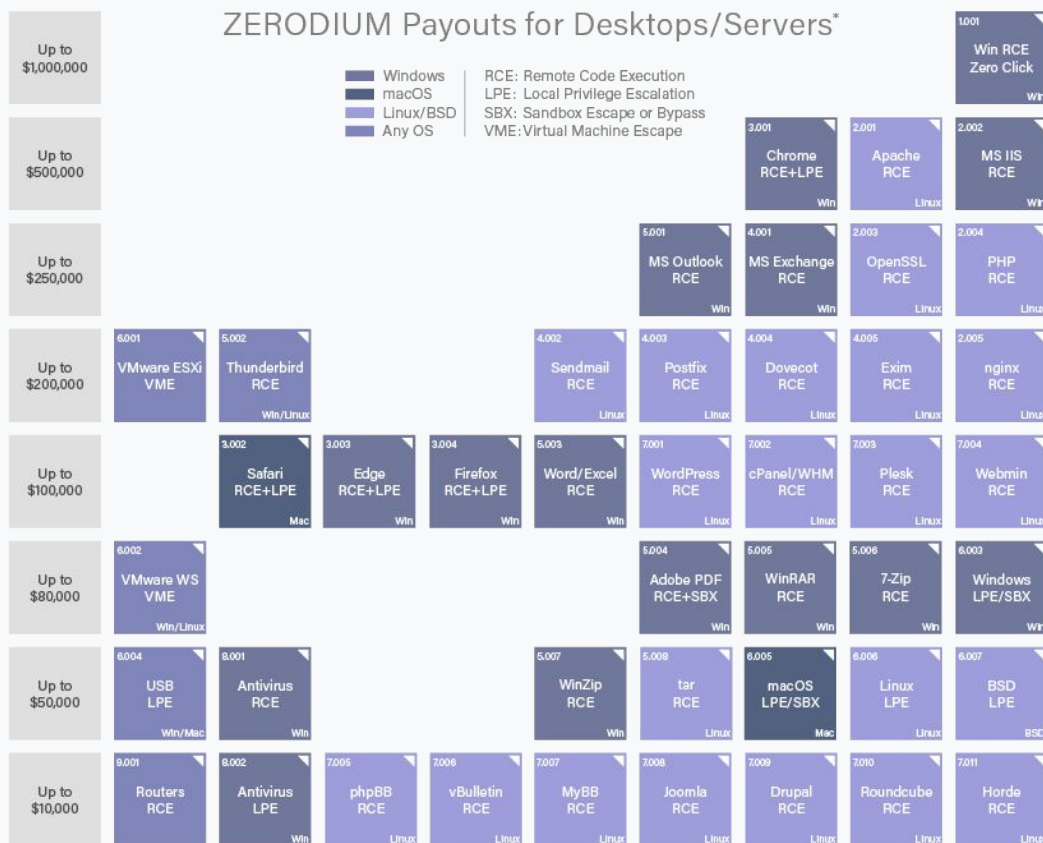
## All software contains bugs!

- Bugs are **errors or flaws** in the program.
- Some bugs can cause apps to crash, others represent **severe security vulnerabilities**.
- Hackers are constantly searching for these bugs.

Hackers have two choices:

1. **Exploit** bugs to hack devices remotely without target interaction (zero-click).
2. **Report** them to software developers and get compensated for it.

# ZERODIUM Payouts for Desktops/Servers\*



\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com



# Preventative Tips



- **Update** device operating system.
- **Update** all apps on device.
- **Do not click** on links from untrusted sources.
- **Limit data** on mobile device.
- Enable **disappearing messages**.
- Enable **Lockdown Mode** (Apple only).
- Enabled **Android Protection Mode** (Android only).
- Get a **second device** (if resources are available).



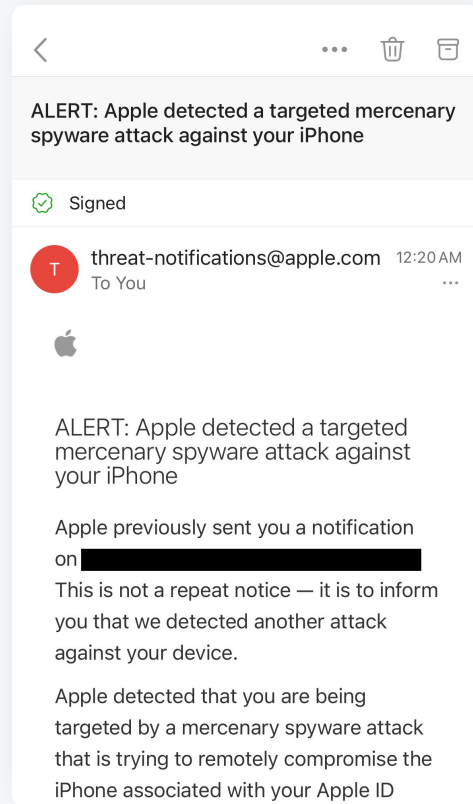
# Responsive Tips



- **Change passwords** for all accounts on the device.
- Enable **two-factor authentication** across accounts.
- **Cover cameras**, especially front-facing ones.
- **Test device** to learn when, what, how.

# Symptoms of a Hack

- Spyware generally presents no **noticeable symptoms**.
- Spyware **infects silently**.
- However, some common complaints from targets have included:
  - Rapid drainage of the phone battery
  - Suspicious behavior from apps
  - Abnormal data usage
  - Receipt of suspicious links or attachments
  - The camera opening without user prompt
- For Apple users, Apple now sends regular threat notifications →



# Testing Devices

## **Citizen Lab:**

<https://citizenlab.ca/spyware-outreach/>

## **Access Now:**

<https://www.accessnow.org/help/>

## **Amnesty Security Lab:**

<https://securitylab.amnesty.org/get-help/>



# 4.

## Protecting Accounts from Hacking

From: "Dropbox Notification" <[dropbox.noreplay@gmail.com](mailto:dropbox.noreplay@gmail.com)>

Date: Dec 7, 2016 [REDACTED]

Subject: You have 1 new file in your inbox

To: [REDACTED]

Cc:



Hi [REDACTED]

You have received a new document in your inbox, view the file "مذكرة القبض على عزة سليمان.pdf" on Dropbox.

[View file](#)

From: "Dropbox Notification" <[dropbox.noreplay@gmail.com](mailto:dropbox.noreplay@gmail.com)>

Date: Dec 7, 2016 [REDACTED]

Subject: You have 1 new file in you


To: [REDACTED]

Cc:

Hi [REDACTED]


You have received a new docu

dropboxsupport.servehttp.com/?rid=[REDACTED]&#identifer



Get the best Dropbox experience on-the-go, for free!

Sign in to Dropbox




[Sign in](#)

☐ Stay signed in [Forgot password?](#)

Dropbox Account for everything

[About Dropbox](#) [Privacy](#) [Terms](#) [Help](#)


 English (United States)

.pdf" on Dropbox.

# How Are Accounts Hacked?

Accounts = email, cloud, social media, etc.

 You fall for a **phishing attempt** (link).

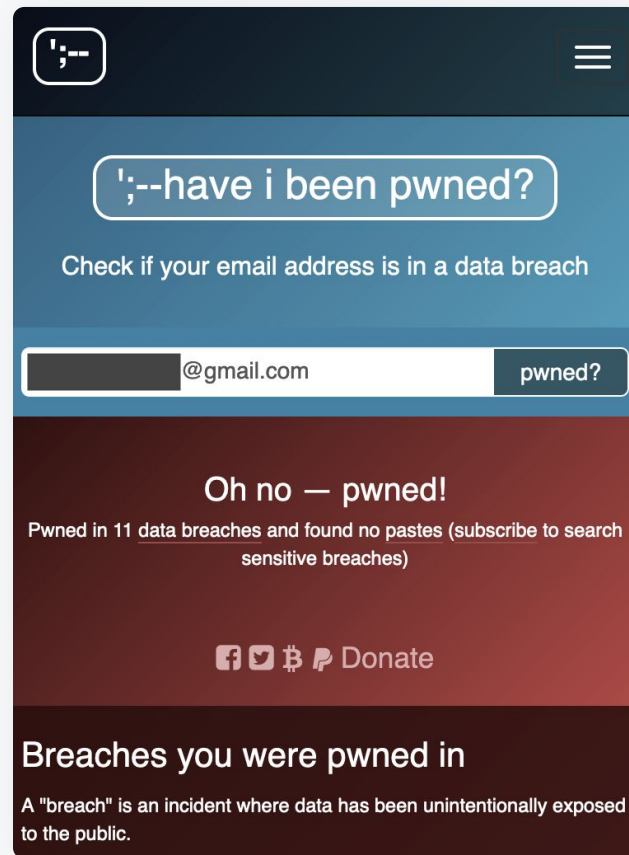
 Your password is **easy** to guess.

 Your password is **already online**: [haveibeenpwned.com](https://haveibeenpwned.com)

# Check for Leaks

- Check whether your account credentials (password, phone number, etc.) have been **leaked** on some hacker forum: <https://haveibeenpwned.com/>

*Note: passwords are not leaked in plaintext but in hashed form.*



# Preventative Tips



- Have a **strong and unique password** for each account.
- Store passwords in a **password manager**.
- Enable **two-factor authentication** (not through SMS).
- Beware of **phishing links**.
- Activate **login alerts** (where available).

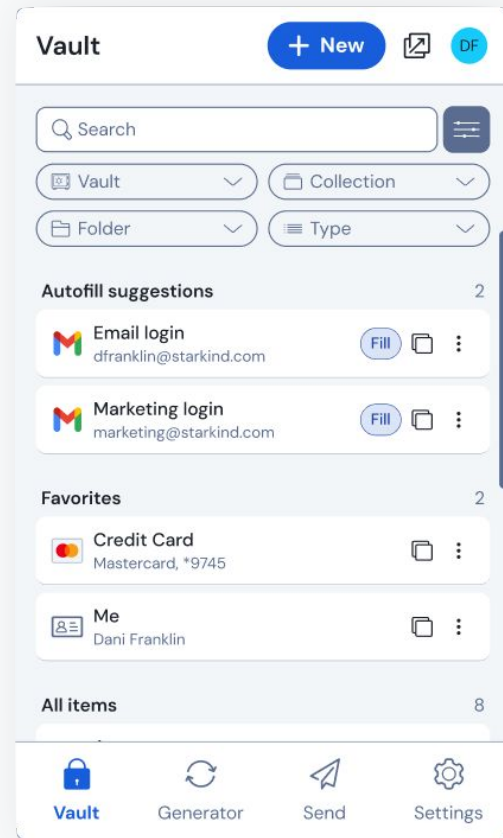


Where do you **store**  
your **account**  
**passwords?**

# Password Managers

- Unreasonable to expect humans to memorize **multiple jumbled characters** for **hundreds of accounts**.
- Store passwords in a secure vault → password managers.
- Password managers can also **generate complex passwords** for you.

The only thing you need to **memorize** is the password to access the password manager.



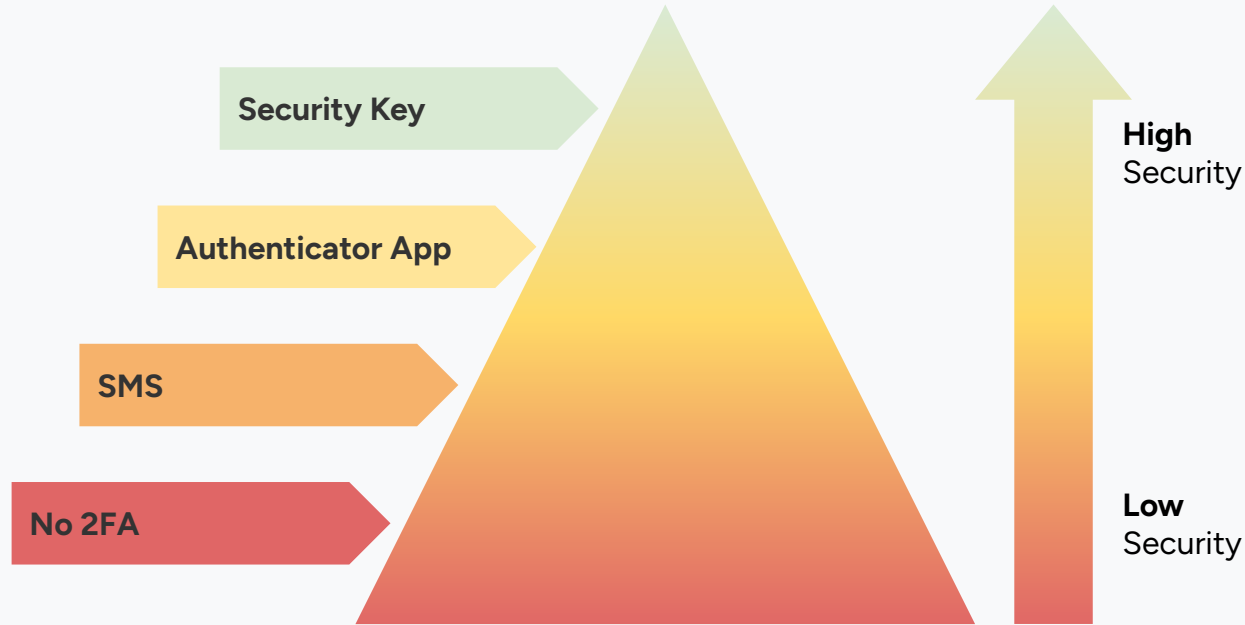


# Two Passwords to Memorize

1. Password to **unlock/access your device** (passcode).
2. Password to **access your password manager**.

You can rely on your password manager to remember all other passwords.

# Two-Factor Authentication



# Make a To-Do List

Service	Is 2FA Enabled?	What Kind of 2FA?	Strong Password?	Stored in Password Manager?
Facebook	✓	Authenticator App	✓	✓
Google	✓	Security Key	✓	✓
X	✓	SMS	✗	✗
Proton	✗	—	✓	✓

# Responsive Tips



→ **Attempt to login again** using the same device and credentials.

**If that doesn't work, try:**

→ Google: <https://g.co/AccountRecoveryRequest>

→ Facebook: <https://www.facebook.com/hacked>

→ Instagram: <https://www.instagram.com/hacked>

→ **Seek support** from a digital security hotline.

# Toolbox Recommendations



## Password Manager

- Bitwarden: [bitwarden.com](https://bitwarden.com)
- KeyPass: [keepassxc.org](https://keepassxc.org)
- Proton Pass: [proton.me/pass](https://proton.me/pass)

## Authenticator App

- Google Authenticator
- FreeOTP: [freeotp.github.io](https://freeotp.github.io)

# 5.

## Search Warrants and Warrantless Searches

# United States

Meta responds to government requests for data in accordance with applicable law and our terms of service. Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague. The charts below provide data on the number of requests we received, the number of users/accounts requested, and the rate we complied with all or some of the government's request.

< Jan - Jun 2024 >

**81,884**

Total requests

**77,603**

Legal process requests

**4,281**

Emergency disclosure requests

**151,328**

Users/accounts requested

**87.90%**

Of requests where some data produced

# Israel

Meta responds to government requests for data in accordance with applicable law and our terms of service. Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague. The charts below provide data on the number of requests we received, the number of users/accounts requested, and the rate we complied with all or some of the government's request.

< Jan - Jun 2024 >

**865**

Total requests

**314**

Legal process requests

**551**

Emergency disclosure requests

**2,657**

Users/accounts requested

**79%**

Of requests where some data produced



Email informing a journalist that the FBI issued a legal process requesting information related to their **Google** account.



usernotice@google.com

to usernotice-noreply ▾



Dear Google User,

Google received and responded to a legal process issued by the Federal Bureau of Investigation compelling the release of information related to your Google account. A court order previously prohibited Google from notifying you of the legal process. We are now permitted to disclose the receipt of the legal process to you. The agency reference number or case number on the legal process is [REDACTED]

For more information about how Google handles legal processes, view our transparency report at <http://www.google.com/transparencyreport/userdatarequests/legalprocess/>.

Google is not in a position to provide you with legal advice or discuss the substance of the legal process. If you have other questions regarding this matter, you may wish to contact an attorney.

Reply directly to this email in any further communications regarding this matter. Any communications not sent as a direct reply to this email must contain the subject line "Attention Google Legal Investigations Support," reference the case identification number, and be sent to [usernotice@google.com](mailto:usernotice@google.com) in order to ensure the appropriate routing and processing.

Regards,  
Legal Investigations Support  
Google LLC



You received this announcement to update you about important information in regards to your Google account.  
© 2023 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



# Why Encryption Matters

- Platforms **frequently comply** with legal requests or state pressure to handover data about users.
- Data can encompass: IP addresses, device information, and potentially even the content of emails, documents, photos, etc.

Data produced depends on whether platform **encrypts data AND metadata** on its servers.

Download results of your legal order on the [WhatsApp Law Enforcement Portal](#)

**Service** WhatsApp

**Account Identifier** [REDACTED]

**Account Type** WhatsAppUser

**Generated** [REDACTED]

**Date Range** [REDACTED]

Message Log: Information about WhatsApp text, audio, image, and video messages sent and received by the account holder

**Message Log Definition** Target IPs and Ports: Text, audio, image, and video messages IP addresses and Port numbers for only the target account holder

Sender IPs and Ports: IP addresses and port numbers for all WhatsApp users involved in sending WhatsApp text, audio, image, and video messages with the target account holder.

**Timestamp** [REDACTED]

**Message Id** [REDACTED]

**Sender** [REDACTED]

**Recipients** [REDACTED]

**Group Id** [REDACTED]

**Message**

**Sender Ip** [REDACTED]

**Sender Port** [REDACTED]


**Sender Device** [REDACTED]

**Type** text

**Message Style** group

**Message Size** 504

**Attachment A**

<b>Account</b>	<b>Responsive Information in Signal's Possession</b>
	Last connection date: 1634169600000 (unix millis)  Account created: 1606866784432 (unix millis)

# Check Transparency Reports

- **Meta:** <https://transparency.meta.com/reports/government-data-requests/>
- **Google:** <https://transparencyreport.google.com/user-data/overview>
- **Proton:** <https://proton.me/legal/transparency>
- **Signal:** <https://signal.org/bigbrother/>

# Preventative Tips



→ Use tools that **encrypt both** data and metadata (e.g. Signal).

→ **Avoid storing** sensitive information on big tech platforms (e.g. Meta, Google, OpenAI, Amazon, etc.).



# Responsive Tips



→ **Archive and delete data** stored on big tech platforms  
(e.g. Google: <https://takeout.google.com>).





# 6.

## Dealing with Doxxing and Harassment

# Ask ChatGPT:

“Tell me everything  
you know about  
[full name].”



🔍 "Khalil Gibran"



Google Search

I'm Feeling Lucky

# Data Brokers

- When searching yourself through a search engine, you might find results pointing to a website run by a **data broker**.
- Data brokers use public records to **aggregate information about you**, including:
  - Current and previous addresses, phone numbers, names of family members, or previous names (if you've changed your name).
- You can **opt out**:

<https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List>



# Preventative Tips



→ Setup **Google Alerts** for your name:

<https://www.google.com/alerts>

→ Request for search results to be **de-indexed**.

→ **Remove personal details** from social media pages  
(phone number, home address, etc.)

→ **Review privacy settings** on social media pages.

→ Opt-out of **data brokers**.

→ Consider creating **pseudonymous identities**.

# Responsive Tips



- **Aggregate** all harassing and doxxing posts: grab screenshots, link to profiles.
- **Report campaign** to a digital security hotline.
- Consider **going offline** temporarily.



# 7.

## Obfuscating Location

# Connecting through HTTP

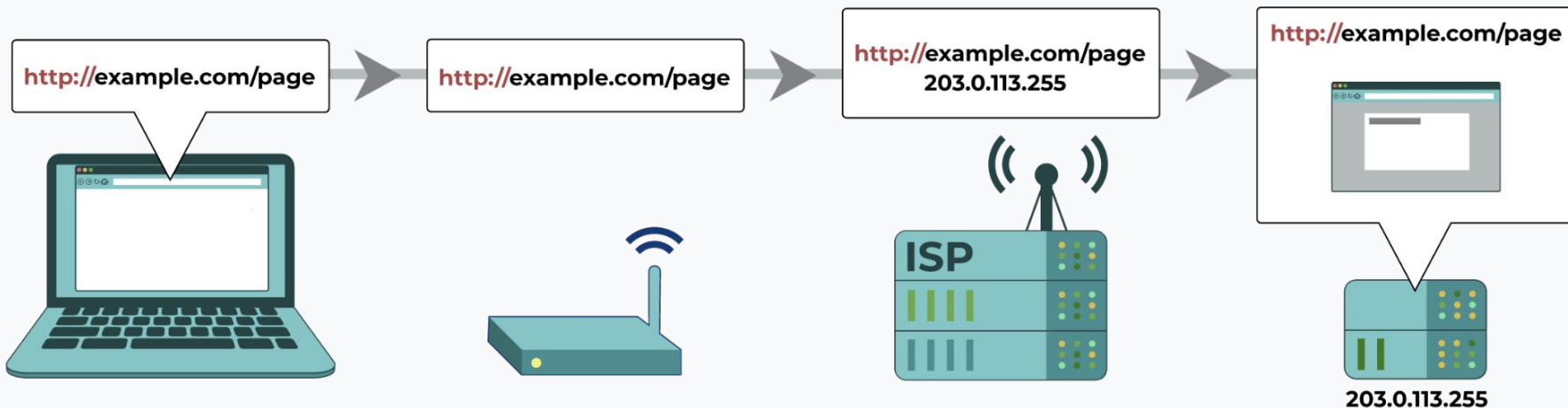


IMAGE SOURCE: EFF.ORG



# Connecting through HTTPS

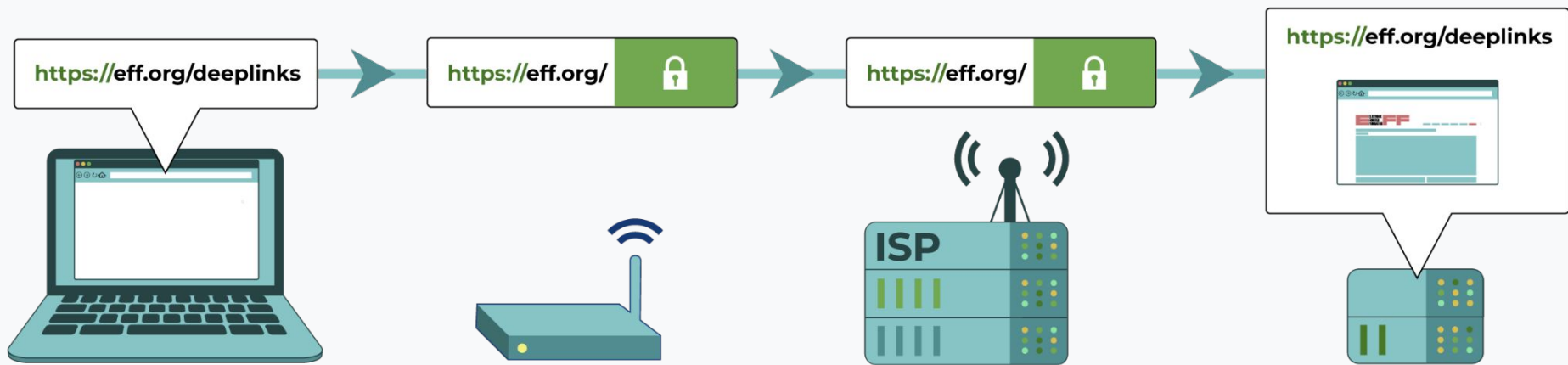


IMAGE SOURCE: EFF.ORG

# Connecting to a Website Through a VPN

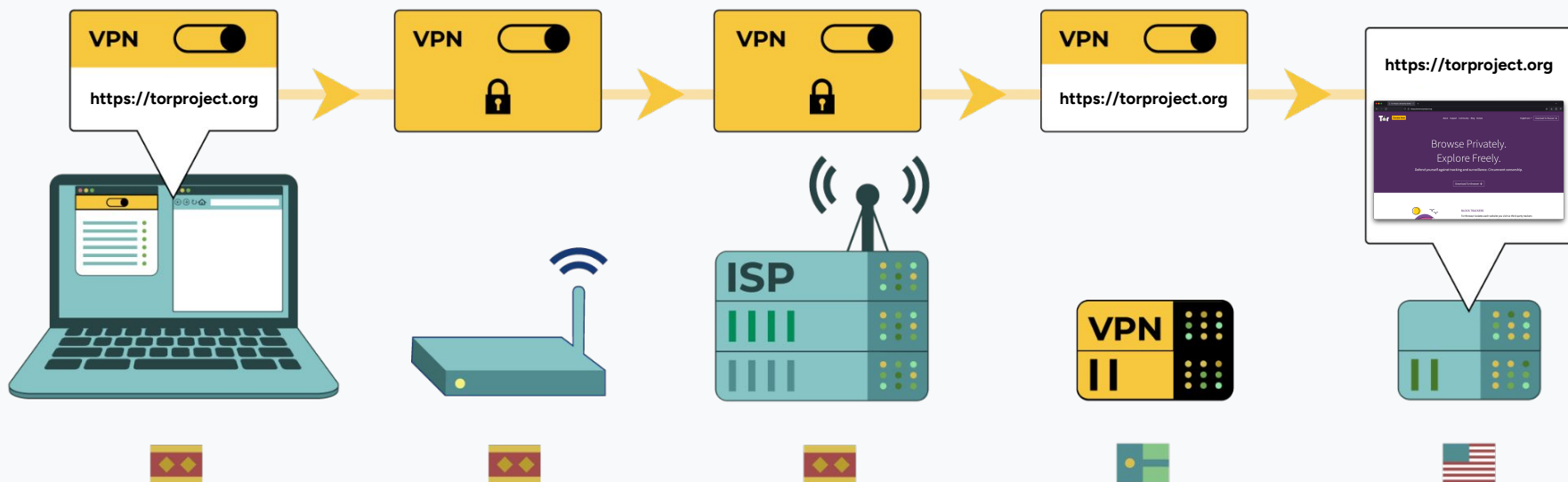


IMAGE SOURCE: EFF.ORG

# Connecting to a Website Through Tor

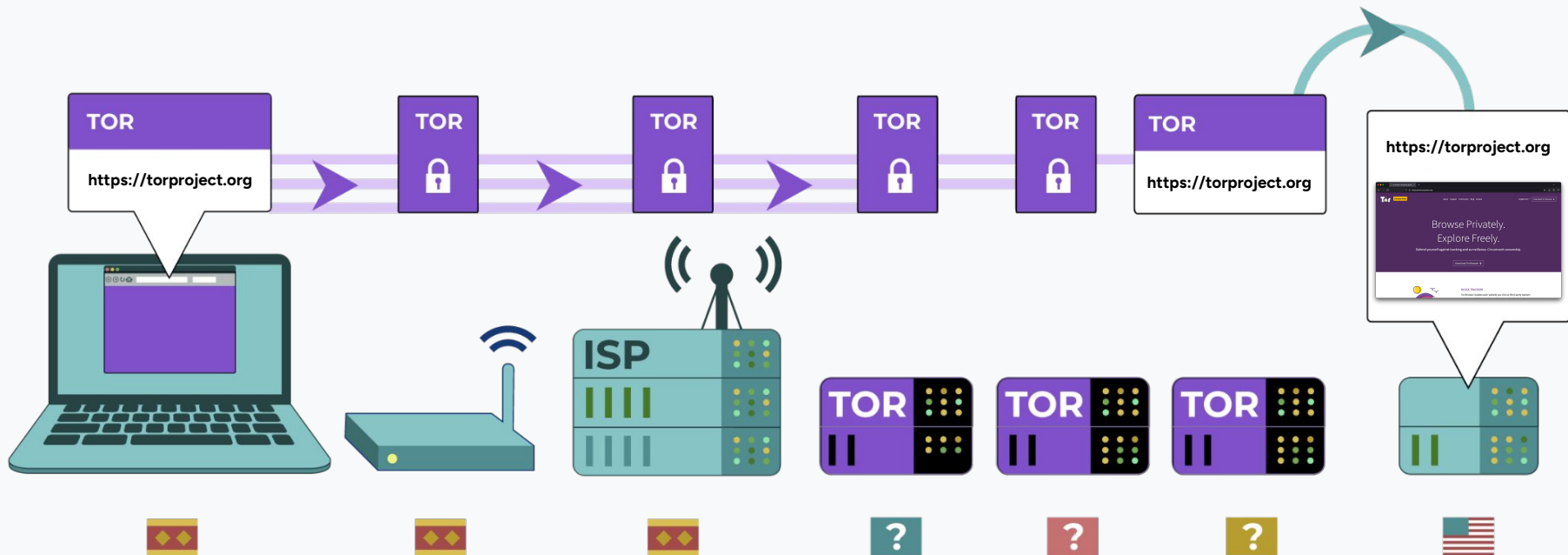


IMAGE SOURCE: EFF.ORG

# Toolbox Recommendations



## Browser

- Mullvad: [mullvad.net](https://mullvad.net)
- Brave: [brave.com](https://brave.com)
- Firefox: [www.mozilla.org/en-US/firefox/new](https://www.mozilla.org/en-US/firefox/new)
- Tor: [torproject.org/download](https://torproject.org/download)

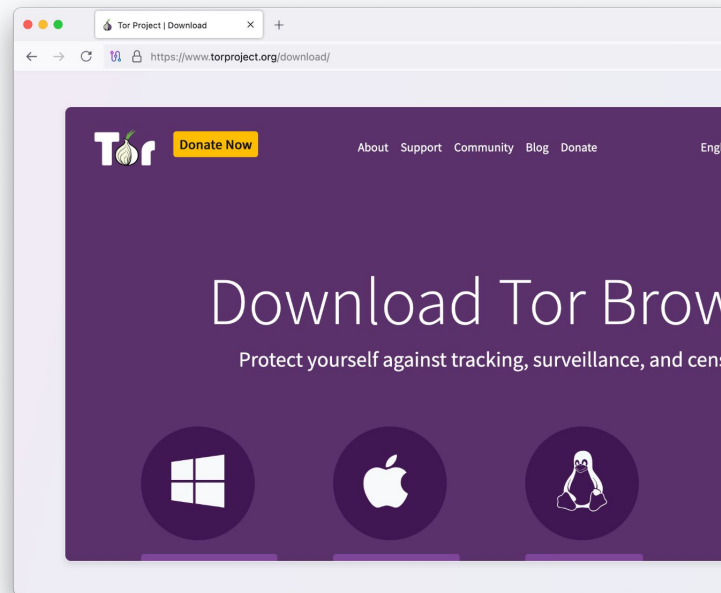
## VPN

- Mullvad: [mullvad.net](https://mullvad.net)
- Psiphon: [psiphon.ca](https://psiphon.ca)
- Proton: [proton.me](https://proton.me)
- Orbot: [orbot.app](https://orbot.app)



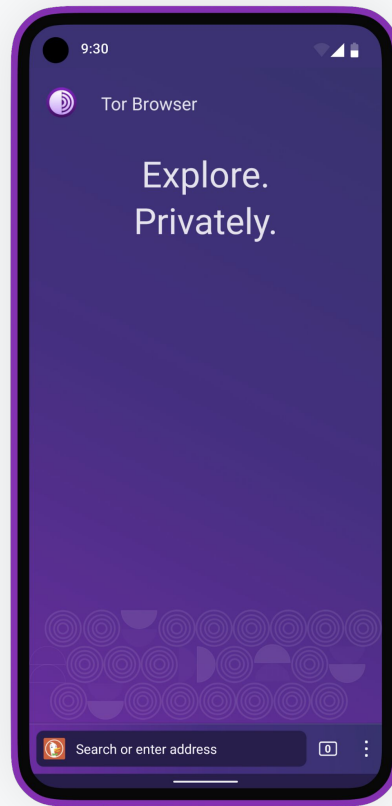
# What is Tor Browser?

- Tor Browser is just like any other browser (Chrome, Firefox, Safari) except it **does not expose who you are and what websites you're visiting** to anyone surveilling your traffic.
- Tor Browser is available in 37 languages in a single **multi-locale** [download](#).
- The Tor Project maintains a [user-friendly guide](#) for novice users which is also multilingual.



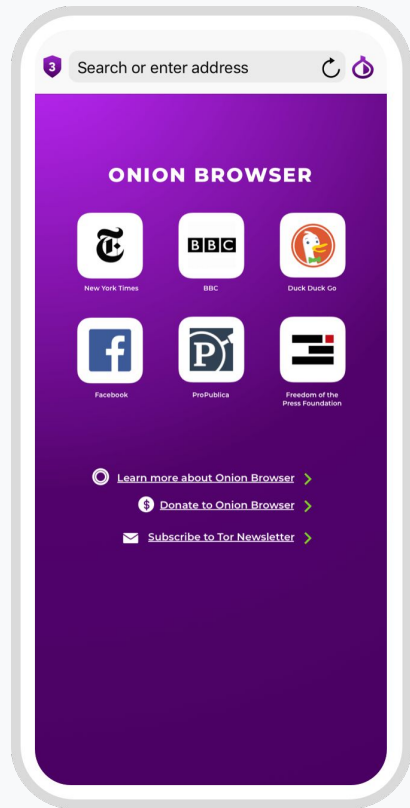
# Tor Browser for Android

- Tor Browser for Android **resembles** Tor Browser for desktop in terms of features and protections. It is developed and maintained by the Tor Project.
- Users can download the application from the **Google Play** or **F-Droid** repository.
- Alternatively, users can download the .apk file from:  
<https://torproject.org/download/>



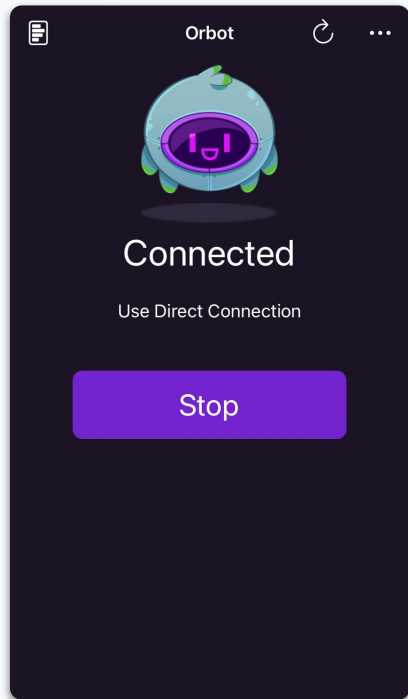
# Onion Browser for iOS

- Onion Browser is the **unofficial Tor browser** for iOS and the only one endorsed by the Tor Project.
- It is also **free and open source**, and is developed and maintained by [The Guardian Project](https://theguardianproject.org/).
- There is no official browser called 'Tor Browser' for iOS → Be careful as **many fake Tor browsers** exist on iOS!
- Onion Browser is available through the Apple App Store:  
<https://onionbrowser.com/>



# Orbot for Android and iOS

- Orbot is a mobile application that essentially routes **all your smartphone's traffic** through Tor, instead of just a browser going through Tor such as with Tor Browser.
- For example, you can **route apps** like Signal through Tor for enhanced privacy and security.
- It is developed and maintained by [The Guardian Project](https://theguardianproject.org/) as free and open-source software, and is available on both iOS and Android:  
<https://orbot.app/>





# What About Mobile Networks?

The following section was adapted from learning resources created by the **Freedom of the Press Foundation**. Learn more here:

[freedom.press/digisec/blog/obfuscating-location-module](https://freedom.press/digisec/blog/obfuscating-location-module)

# What Makes a Phone, a Phone?

- Smartphones have at least **three wireless transmitters** and **receivers**:
  - Cellular (GSM, CDMA)
  - WiFi
  - Bluetooth
- Smartphones also have **GPS**, but that is only one part of what contributes to finding your position.

# Cell Tower Triangulation

- Location based on distance from **3+ nearby cell towers**.
- Based on device strength, round-trip signal time.
- The more tower density (e.g. in cities), the more specific the location.

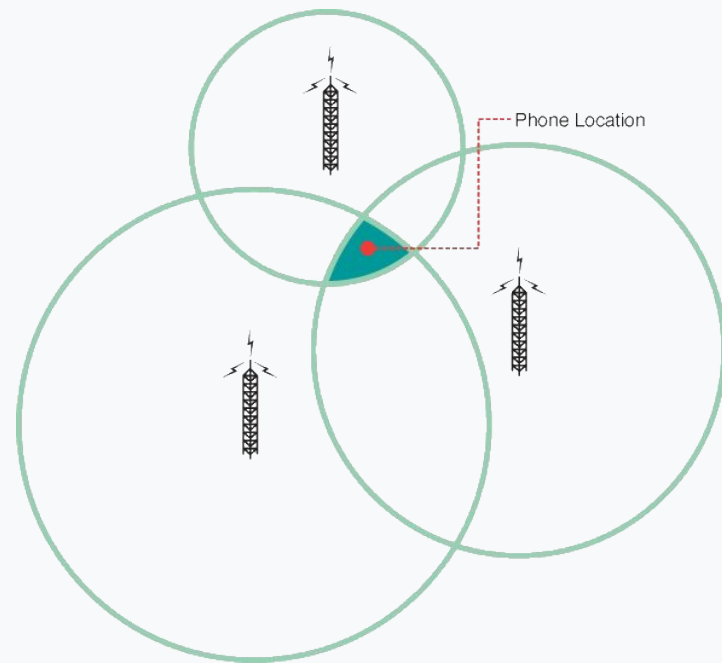


IMAGE SOURCE: O'REILLY

# WiFi Positioning System

- Similarly, WiFi databases (e.g., Wigle.net location service) log the relative location of WiFi routers.
- When WiFi is enabled, your device may check location in a Wi-Fi positioning database.

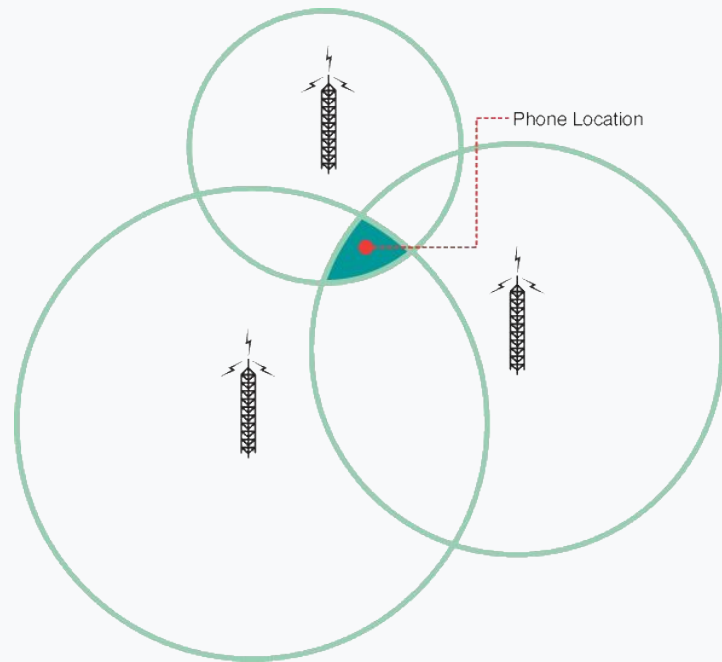


IMAGE SOURCE: O'REILLY

# Global Positioning System (GPS)

- There are **31 navigation satellites** circling the Earth.
- Your device receives signals from 4+ GPS satellites, and calculates distance from each one.
- Depending on the receiver, can be accurate to a few yards, or even inches.



# What to Do with Cell Phones?

- We have to understand that this is a risk with all mobile phones.
- **If it's on, the phone company gets the location.**
  - That provider may be compelled to share your location data, if they receive a legal request.
- Is this a problem? Depends on your threat model.
  - When broadcasting your location is a problem, you *could* leave your phone at home.
  - ... But what's the tradeoff of *not* bringing it? What if you need it for something? That will depend on your particular situation.

# What to Do with Cell Phones?

- If you really need it in the future, you may be equipped to access a **temporary phone**, that is not tied to you.
- The longer you use two phones in the same place, the more the two devices look like they are **tied to the same person**.
  - If this is a problem for you, keep them separated when possible.



# Toolbox Recommendations



→ Placing devices inside **Faraday pouches** takes them off the grid, making them unable to send or receive any signals.



# 8.

## Secure Communication

# Without Encryption



Example: SMS, phone calls

IMAGE SOURCE: EFF.ORG

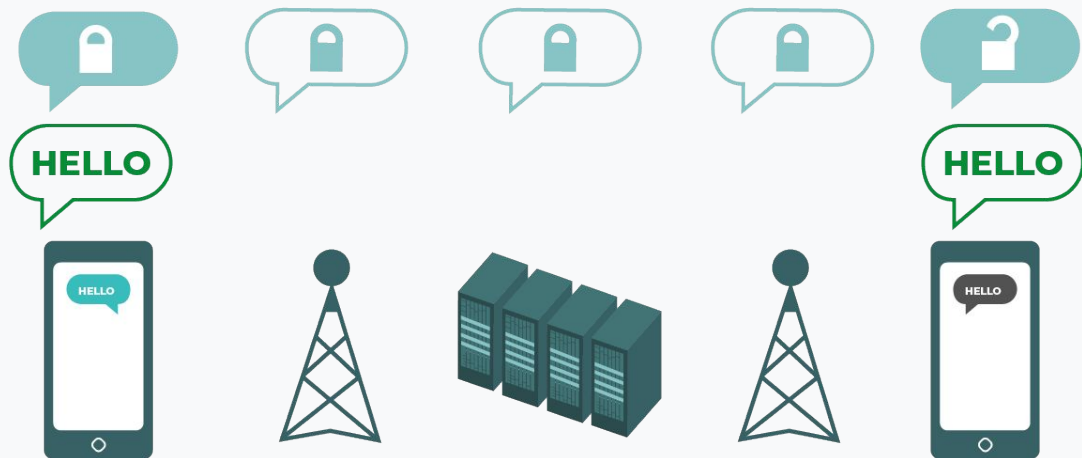
# Some Encryption



Example: email (sometimes), Telegram, Instagram DMs, Twitter DMs, etc.

IMAGE SOURCE: EFF.ORG

# End-to-End Encryption



Example: Signal, WhatsApp (partly)

IMAGE SOURCE: EFF.ORG

# Toolbox Recommendations



## Messaging

- Signal: [signal.org](https://signal.org)
- Simplex: [simplex.chat](https://simplex.chat)
- Element: [element.io](https://element.io)



# More Toolbox Recommendations



## Search Engine

- DuckDuckGo: [duckduckgo.com](https://duckduckgo.com)
- Mullvad Leta: [leta.mullvad.net](https://leta.mullvad.net)
- StartPage: [startpage.com](https://startpage.com)

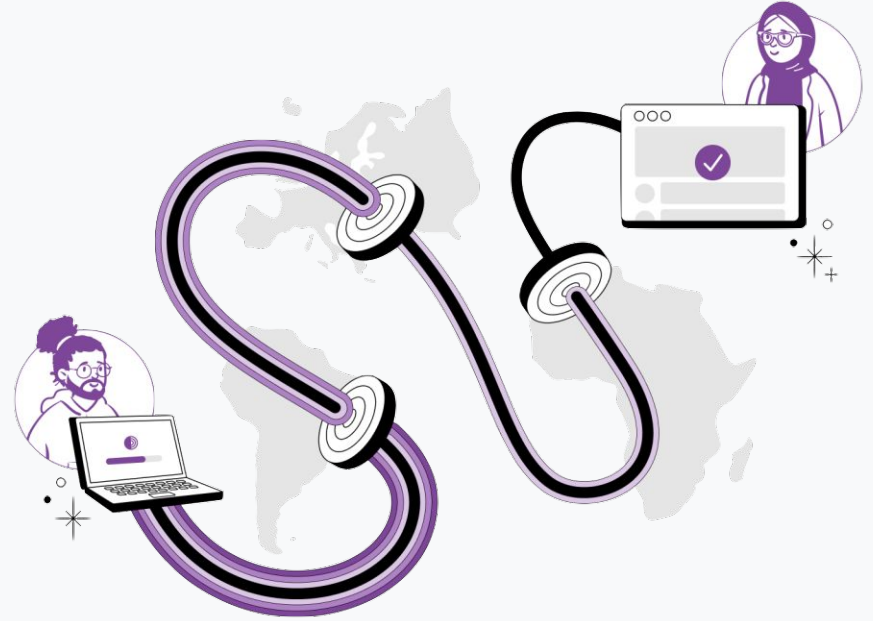
## Storage

- Proton Drive: [proton.me/drive](https://proton.me/drive)
- Tresorit: [tresorit.com](https://tresorit.com)
- Offline storage (USBs and hard drives)

## Email

- Protonmail: [proton.me/mail](https://proton.me/mail)
- Riseup Mail: [riseup.net](https://riseup.net)
- Tuta: [tuta.com](https://tuta.com)

# Thank you!





# The Tor Project Support Channels

**Signal:** <https://signal.me/#p/+17787431312>

**Email:** [frontdesk@torproject.org](mailto:frontdesk@torproject.org)

**WhatsApp:** <https://wa.me/447421000612>

**Telegram:** <https://t.me/torprojectsupportbot>

**Forum:** <https://forum.torproject.org>

