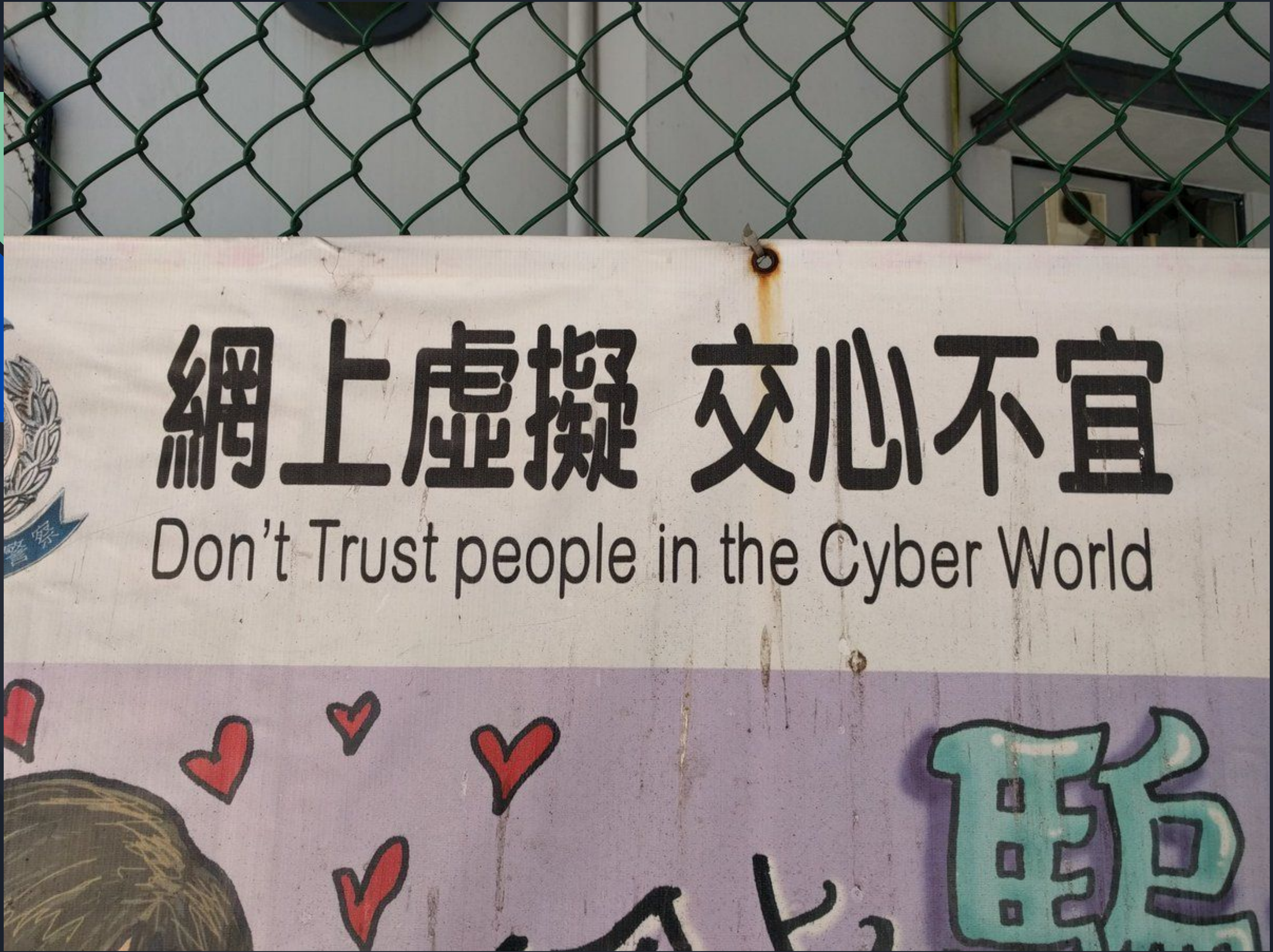
Digital Deadbolt: Securing Yourself Online

Version 5.3
Updated: September 2020
By: Sam Smith


網上虛擬 交心不宜
Don’t Trust people in the Cyber World
警察

Which video conferencing tool is right for the job?

Service	Supports end-to-end encryption?	Supports self-hosting?	Need to register an account to join meetings?	Meeting capacity (free version)
Zoom	✗	✓ (Except call metadata)	Not required (Web only)	100
Google Hangouts (consumer)	✗	✗	Required	25
Google Meet (business)	✗	✗	Not required	250 (Paid versions only)
Skype	✗	✗	Not required	50
Microsoft Teams	✗	✗	Not required	250 (Paid versions only)
Slack	✗	✗	Required	15 (Desktop only)
Webex	✓ (Optional)	✓	Not required	100
Jitsi Meet	Kind of! (2 people)	✓ (Optional)	Not required	75 (Big performance hit)
Whereby (was Appear.in)	Kind of! (4 people)	✗	Not required	4
FaceTime	✓	✗	Required (Except iPhone)	32 (Apple devices only)
Signal	✓	✗	Required	2
WhatsApp	✓	✗	Required	4
Wire	✓	✓	Not required	4

Current as of April 23, 2020. Please see freedom.press/training/videoconferencing-tools for updates.
See something wrong? Let us know at freedom.press/contact

FREEDOM OF THE
PRESS FOUNDATION

WHILE WE WAIT PLEASE DOWNLOAD!

MAC USERS

☑ Tor Browser
☑ MalwareBytes
☑ Tunnelbear or Mullvad VPN or ProtonVPN (free)
☑ Browser extensions: HTTPS Everywhere and Privacy Badger
☑ Signal Desktop
☑ GPG TOOLS

IPHONE USERS

☑ Signal
☑ Pixlmet
☑ Tunnelbear
☑ DuckDuckGo

PC USERS

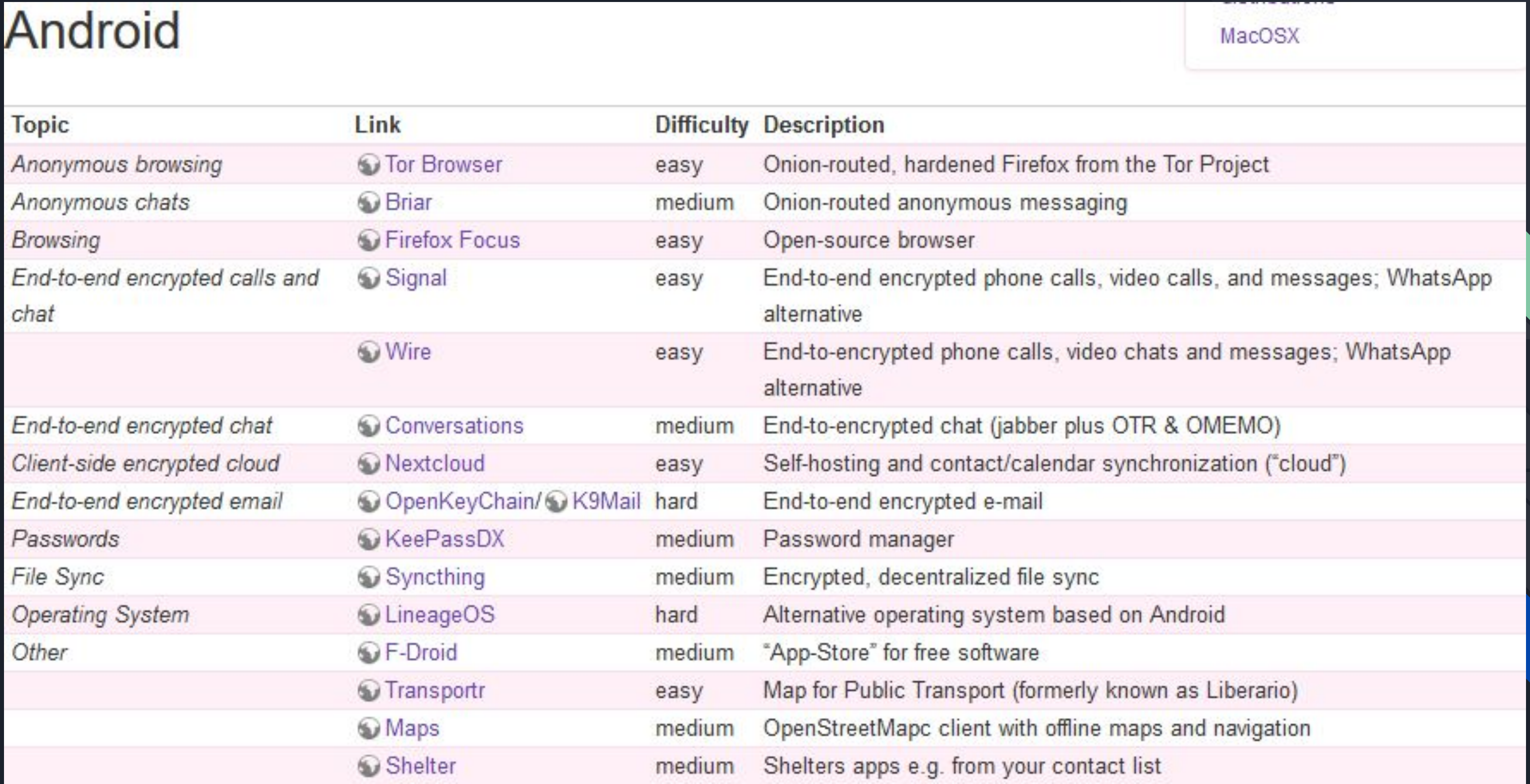
☑ Tor Browser
☑ MalwareBytes
☑ Tunnelbear or Mullvad VPN or ProtonVPN (free)
☑ Browser extensions: HTTPS Everywhere and Privacy Badger
☑ Signal Desktop
☑ GPG FOR WIN
☑ Veracrypt

ANDROID USERS

☑ Signal
☑ Orfox
☑ MalwareBytes
☑ Applock from Domobile
☑ Tunnelbear
☑ DuckDuckGo

https://www.cryptoparty.in/learn/links

Android

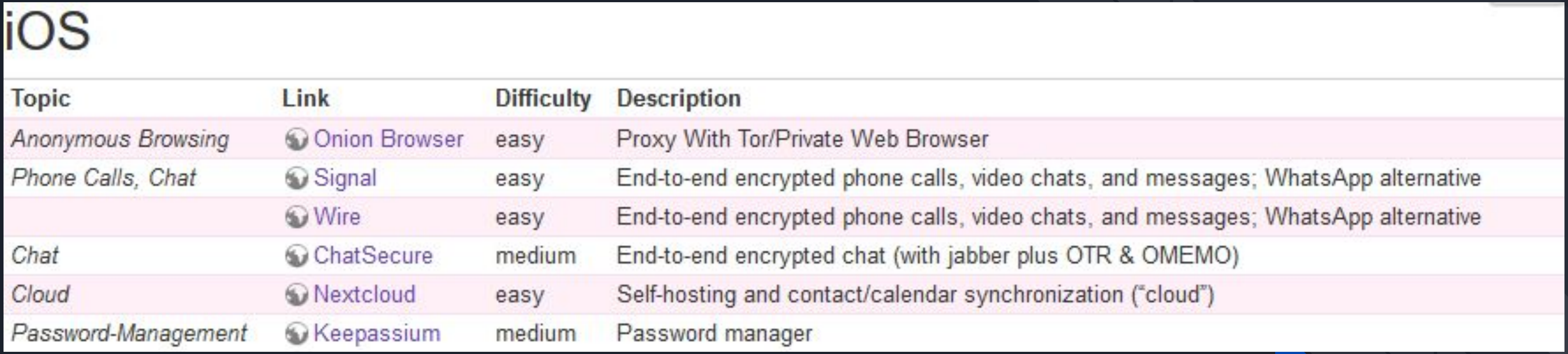


Android

MacOSX

Topic	Link	Difficulty	Description
Anonymous browsing	Tor Browser	easy	Onion-routed, hardened Firefox from the Tor Project
Anonymous chats	Briar	medium	Onion-routed anonymous messaging
Browsing	Firefox Focus	easy	Open-source browser
End-to-end encrypted calls and chat	Signal	easy	End-to-end encrypted phone calls, video calls, and messages; WhatsApp alternative
	Wire	easy	End-to-encrypted phone calls, video chats and messages; WhatsApp alternative
End-to-end encrypted chat	Conversations	medium	End-to-encrypted chat (jabber plus OTR & OMEMO)
Client-side encrypted cloud	Nextcloud	easy	Self-hosting and contact/calendar synchronization ("cloud")
End-to-end encrypted email	OpenKeyChain/ K9Mail	hard	End-to-end encrypted e-mail
Passwords	KeePassDX	medium	Password manager
File Sync	Syncthing	medium	Encrypted, decentralized file sync
Operating System	LineageOS	hard	Alternative operating system based on Android
Other	F-Droid	medium	"App-Store" for free software
	Transportr	easy	Map for Public Transport (formerly known as Liberario)
	Maps	medium	OpenStreetMapc client with offline maps and navigation
	Shelter	medium	Shelters apps e.g. from your contact list

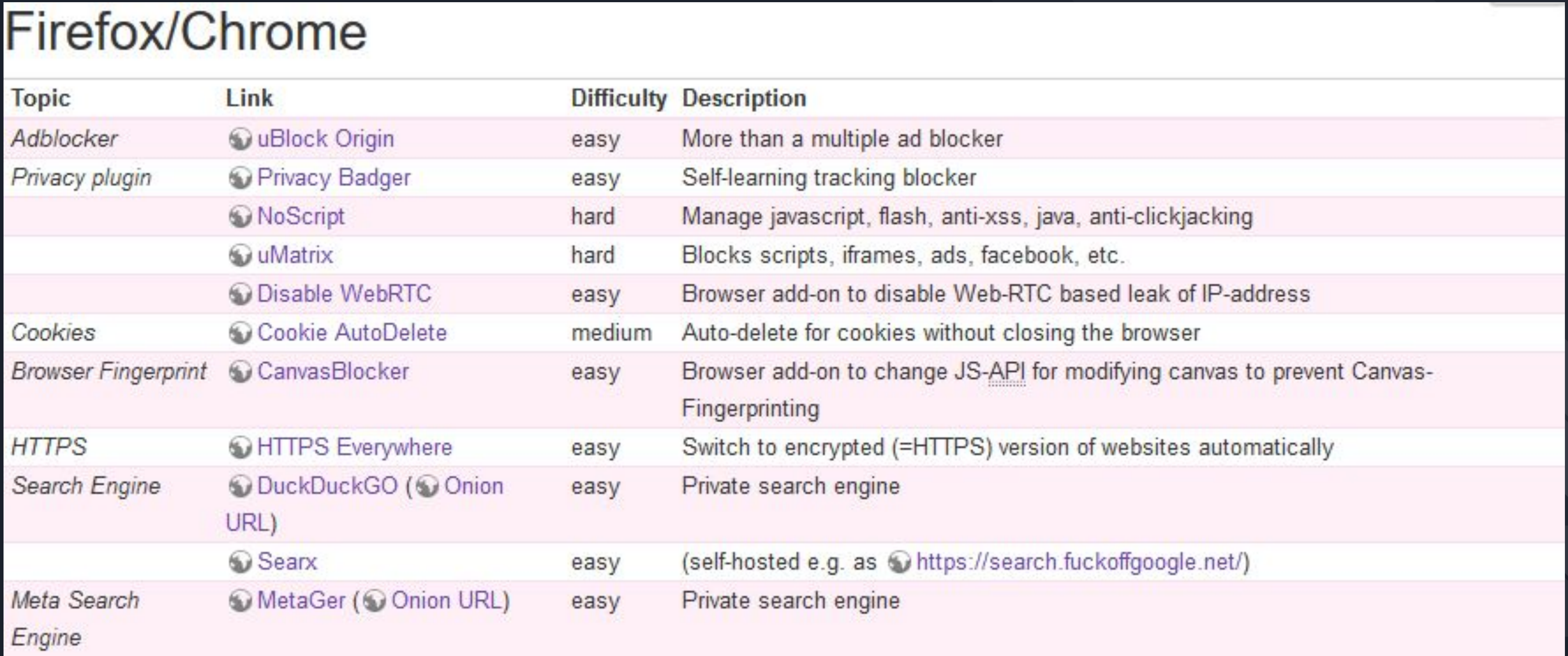
iOS



iOS

Topic	Link	Difficulty	Description
Anonymous Browsing	Onion Browser	easy	Proxy With Tor/Private Web Browser
Phone Calls, Chat	Signal	easy	End-to-end encrypted phone calls, video chats, and messages; WhatsApp alternative
	Wire	easy	End-to-end encrypted phone calls, video chats, and messages; WhatsApp alternative
Chat	ChatSecure	medium	End-to-end encrypted chat (with jabber plus OTR & OMEMO)
Cloud	Nextcloud	easy	Self-hosting and contact/calendar synchronization ("cloud")
Password-Management	Keepassium	medium	Password manager

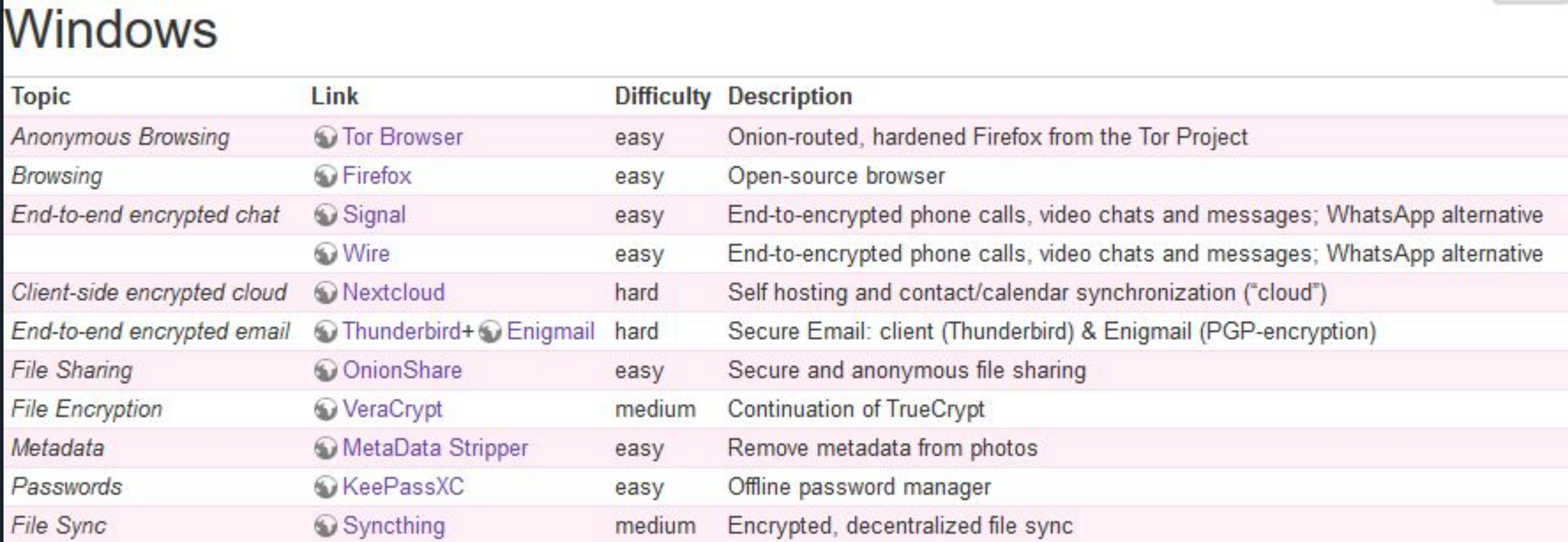
Firefox/Chrome Addons



Firefox/Chrome

Topic	Link	Difficulty	Description
Adblocker	uBlock Origin	easy	More than a multiple ad blocker
Privacy plugin	Privacy Badger	easy	Self-learning tracking blocker
	NoScript	hard	Manage javascript, flash, anti-xss, java, anti-clickjacking
	uMatrix	hard	Blocks scripts, iframes, ads, facebook, etc.
	Disable WebRTC	easy	Browser add-on to disable Web-RTC based leak of IP-address
Cookies	Cookie AutoDelete	medium	Auto-delete for cookies without closing the browser
Browser Fingerprint	CanvasBlocker	easy	Browser add-on to change JS-API for modifying canvas to prevent Canvas-Fingerprinting
HTTPS	HTTPS Everywhere	easy	Switch to encrypted (=HTTPS) version of websites automatically
Search Engine	DuckDuckGO (Onion URL)	easy	Private search engine
	Searx	easy	(self-hosted e.g. as https://search.fuckoffgoogle.net/)
Meta Search Engine	MetaGer (Onion URL)	easy	Private search engine

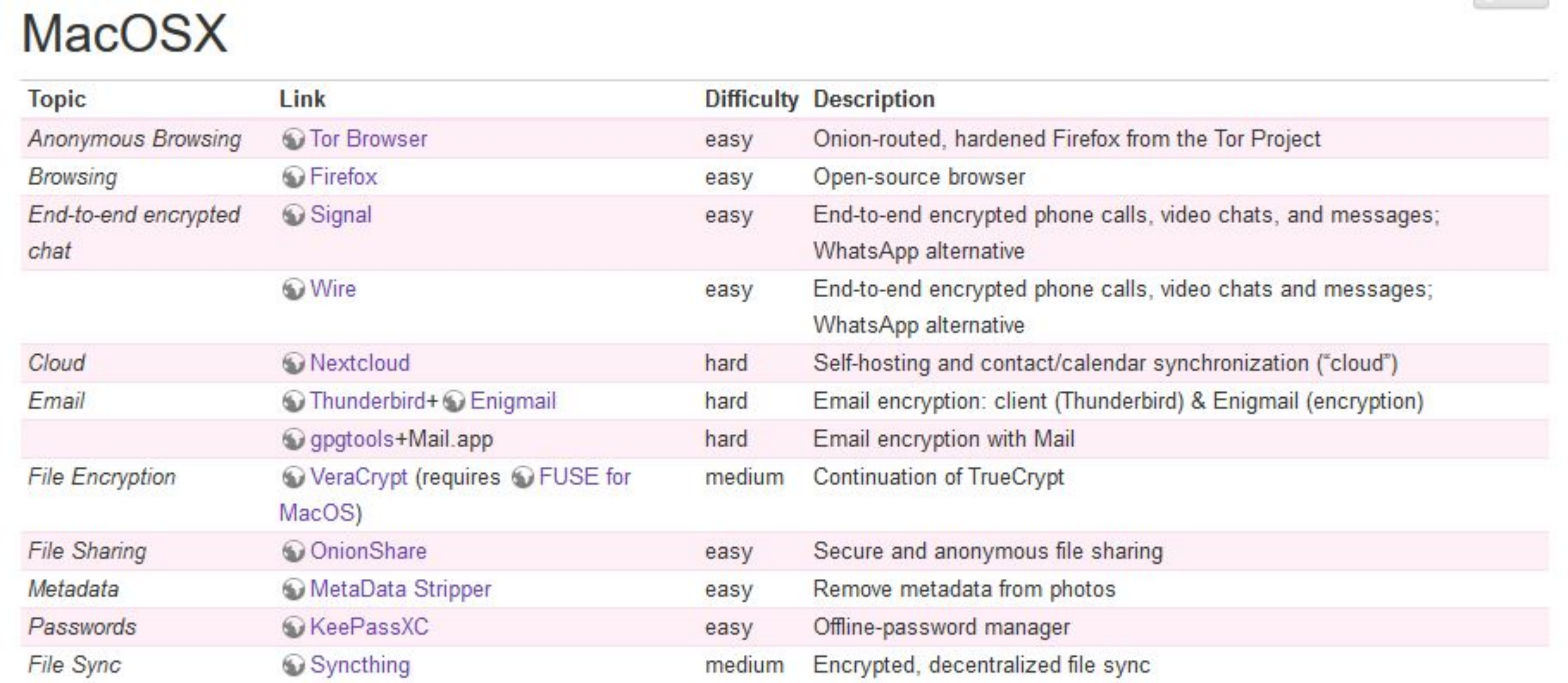
Windows Tools



Windows

Topic	Link	Difficulty	Description
Anonymous Browsing	Tor Browser	easy	Onion-routed, hardened Firefox from the Tor Project
Browsing	Firefox	easy	Open-source browser
End-to-end encrypted chat	Signal	easy	End-to-encrypted phone calls, video chats and messages; WhatsApp alternative
	Wire	easy	End-to-encrypted phone calls, video chats and messages; WhatsApp alternative
Client-side encrypted cloud	Nextcloud	hard	Self hosting and contact/calendar synchronization ("cloud")
End-to-end encrypted email	Thunderbird+ Enigmail	hard	Secure Email: client (Thunderbird) & Enigmail (PGP-encryption)
File Sharing	OnionShare	easy	Secure and anonymous file sharing
File Encryption	VeraCrypt	medium	Continuation of TrueCrypt
Metadata	MetaData Stripper	easy	Remove metadata from photos
Passwords	KeePassXC	easy	Offline password manager
File Sync	Syncthing	medium	Encrypted, decentralized file sync

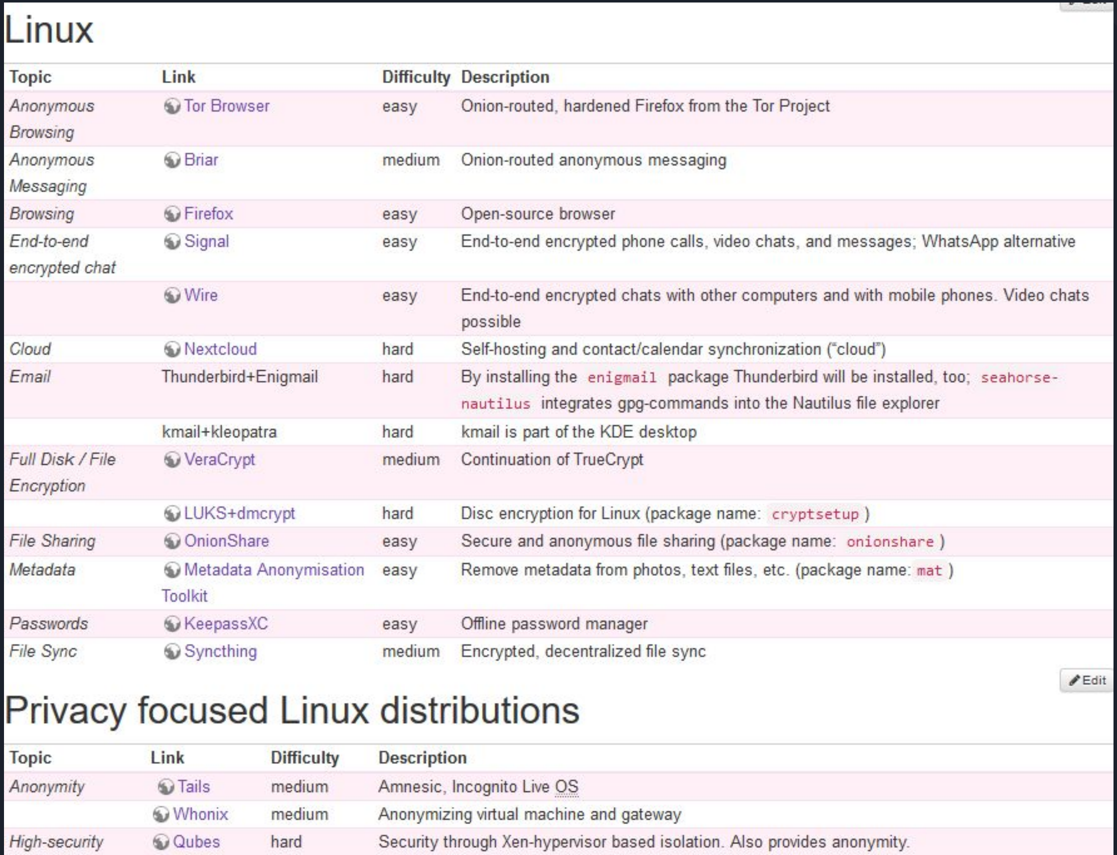
MacOS Tools



MacOSX

Topic	Link	Difficulty	Description
Anonymous Browsing	Tor Browser	easy	Onion-routed, hardened Firefox from the Tor Project
Browsing	Firefox	easy	Open-source browser
End-to-end encrypted chat	Signal	easy	End-to-end encrypted phone calls, video chats, and messages; WhatsApp alternative
	Wire	easy	End-to-end encrypted phone calls, video chats and messages; WhatsApp alternative
Cloud	Nextcloud	hard	Self-hosting and contact/calendar synchronization ("cloud")
Email	Thunderbird+ Enigmail	hard	Email encryption: client (Thunderbird) & Enigmail (encryption)
	gpgtools+Mail.app	hard	Email encryption with Mail
File Encryption	VeraCrypt (requires FUSE for MacOS)	medium	Continuation of TrueCrypt
File Sharing	OnionShare	easy	Secure and anonymous file sharing
Metadata	MetaData Stripper	easy	Remove metadata from photos
Passwords	KeePassXC	easy	Offline-password manager
File Sync	Syncthing	medium	Encrypted, decentralized file sync

Linux Tools



Linux

Topic	Link	Difficulty	Description
Anonymous Browsing	Tor Browser	easy	Onion-routed, hardened Firefox from the Tor Project
Anonymous Messaging	Briar	medium	Onion-routed anonymous messaging
Browsing	Firefox	easy	Open-source browser
End-to-end encrypted chat	Signal	easy	End-to-end encrypted phone calls, video chats, and messages; WhatsApp alternative
	Wire	easy	End-to-end encrypted chats with other computers and with mobile phones. Video chats possible
Cloud	Nextcloud	hard	Self-hosting and contact/calendar synchronization ("cloud")
Email	Thunderbird+Enigmail	hard	By installing the `enigmail` package Thunderbird will be installed, too; `seahorse-nautilus` integrates gpg-commands into the Nautilus file explorer
	kmail+kleopatra	hard	kmail is part of the KDE desktop
Full Disk / File Encryption	VeraCrypt	medium	Continuation of TrueCrypt
	LUKS+dmcrypt	hard	Disc encryption for Linux (package name: `cryptsetup`)
File Sharing	OnionShare	easy	Secure and anonymous file sharing (package name: `onionshare`)
Metadata	Metadata Anonymisation Toolkit	easy	Remove metadata from photos, text files, etc. (package name: `mat`)
Passwords	KeepassXC	easy	Offline password manager
File Sync	Syncthing	medium	Encrypted, decentralized file sync

Privacy focused Linux distributions

Topic	Link	Difficulty	Description
Anonymity	Tails	medium	Amnesic, Incognito Live OS
	Whonix	medium	Anonymizing virtual machine and gateway
High-security	Qubes	hard	Security through Xen-hypervisor based isolation. Also provides anonymity.

In 2018, data surpassed oil in value. Making it the most valuable resource on earth.

The Internet is Bad

The Digital Security Landscape

Risk Analysis

Committee to Protect Journalists Journalists Security Guide - Information Security by Danny O’Brien - hopefully a CryptoParty will clearly explain most of the software and techniques mentioned in this guide.

Your emphasis should be on simplicity. There’s no point in surrounding yourself with computer security that you don’t use, or that fails to address a weaker link elsewhere. Take advantage of what you know well: the people who are most likely to take offense or otherwise target your work, and what they may be seeking to obtain or disrupt. Use that knowledge to determine what you need to protect and how. Ask yourself: What information should I protect? What data is valuable to me or a potential adversary? It might not be what you think of at first. Many journalists feel that what they are doing is largely transparent, and that they have nothing to hide. But think about the dangers to sources if the information they have provided to you was more widely known. What may seem innocuous personal information to you might be incriminatory to others.

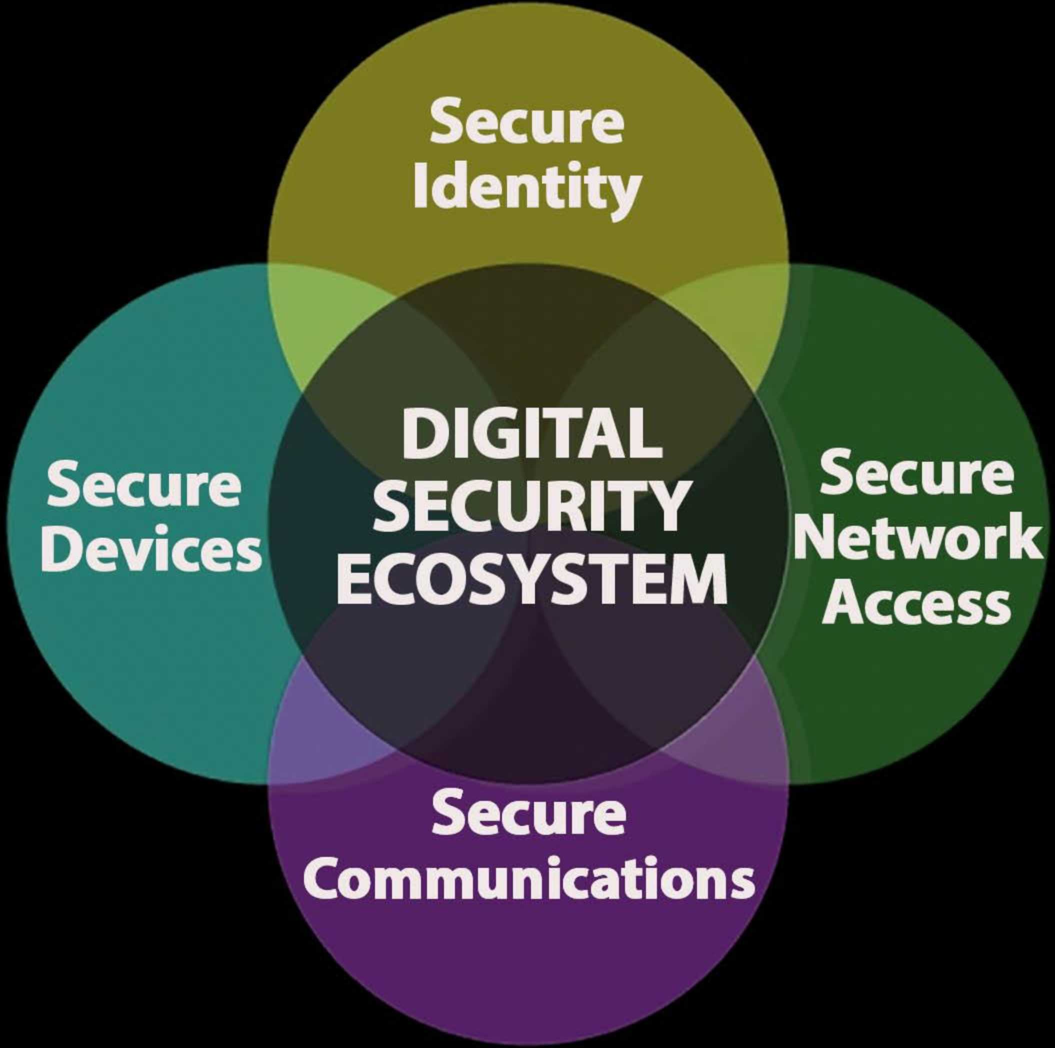
Kerckhoffs's principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. (Kerckhoffs's principle)

This principle should apply to all of the tools and resources mentioned on this page.

Why there is no 100% anonymity

- **People make mistakes** and even the slightest mistake will break the “completeness” of anonymity. (e.g. simply forgetting to turn a proxy on or mentioning the weather)
- **Behavior can be analyzed** (e.g. slang and idioms may locate you).
- **Behavior can be correlated** (e.g when you are home vs online)
- You have to connect somehow. Everything between your body and **your means of anonymity is exposed**. (e.g if you're using tor, *what* you do while using tor may be hidden - that you are *using* tor not, however)
- Some **offline threat** may out you. (e.g. Rubber-hose cryptanalysis)



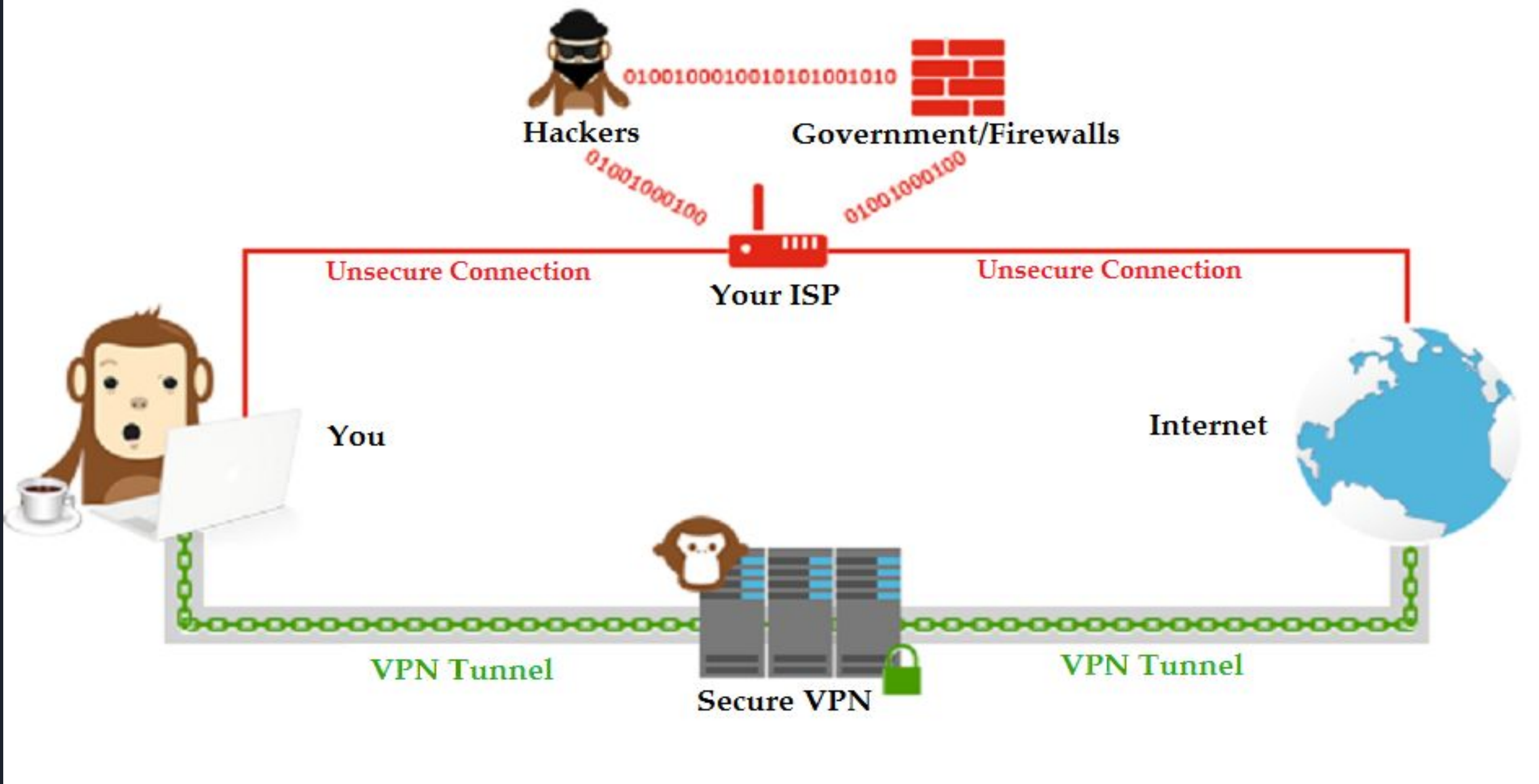
Secure Identity

Secure Devices

DIGITAL SECURITY ECOSYSTEM

Secure Network Access

Secure Communications

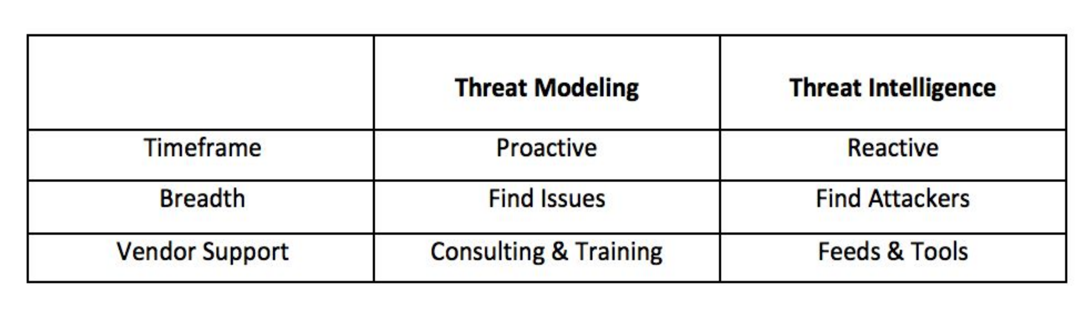

Hackers
01001000100101010100101O
Government/Firewalls
01001000100
01001000100
Unsecure Connection
Your ISP
Unsecure Connection
You
Internet
VPN Tunnel
Secure VPN
VPN Tunnel

TOWARDS DIGITAL RESILIENCE

- Assessment
- Infrastructure
- Training
- Opposition Research
- Crisis Communications

How Do You Manage Risk?

Threat Modeling

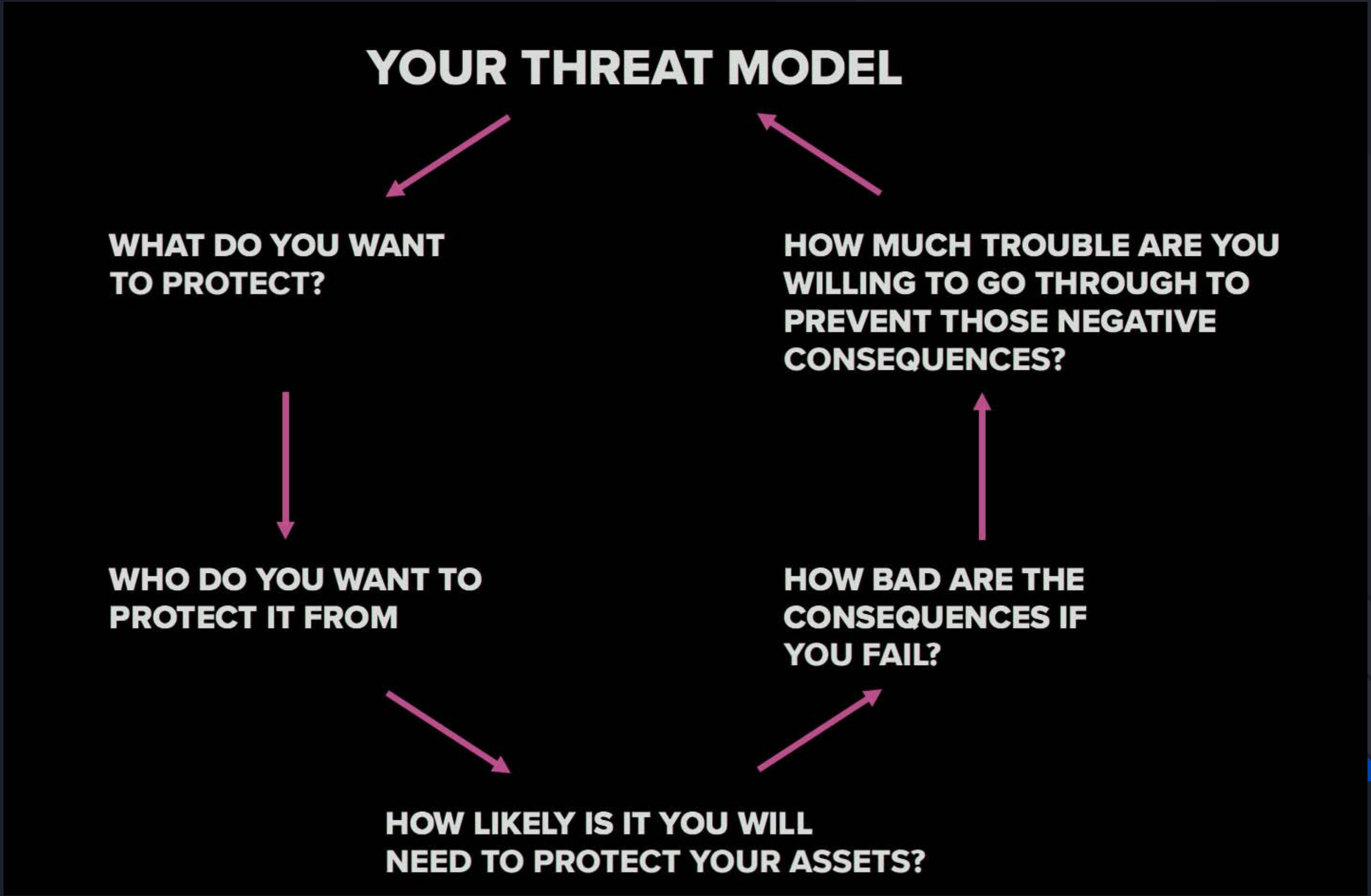


	Threat Modeling	Threat Intelligence
Timeframe	Proactive	Reactive
Breadth	Find Issues	Find Attackers
Vendor Support	Consulting & Training	Feeds & Tools

THREAT MODELING helps you identify threats to the things you value and who you need to protect them from. When building a threat model, you can ask yourself the following questions.

- What do I want to protect?
- Who do I want to protect it from?
- What are the consequences if I fail?
- How likely are these consequences?
- How can I address the most likely risks?

Your chances of getting killed by a cow are low, but never zero



YOUR THREAT MODEL

WHAT DO YOU WANT TO PROTECT?

WHO DO YOU WANT TO PROTECT IT FROM

HOW LIKELY IS IT YOU WILL NEED TO PROTECT YOUR ASSETS?

HOW BAD ARE THE CONSEQUENCES IF YOU FAIL?

HOW MUCH TROUBLE ARE YOU WILLING TO GO THROUGH TO PREVENT THOSE NEGATIVE CONSEQUENCES?

YOU ARE ONLY AS SECURE AS YOUR WEAKEST LINK

RISK ASSESSMENT

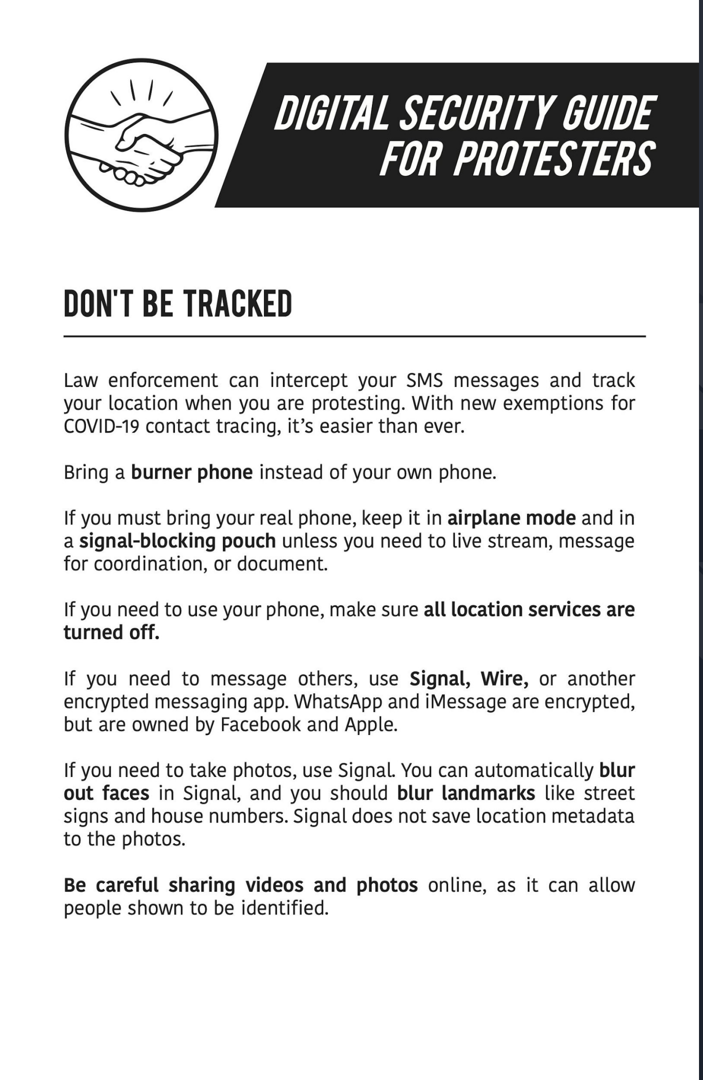
Threats	Adversaries	Vulnerabilities	Current Capacities	Capacities Required
someone accessing your accounts	Roomies, “friends”, infiltrators	sharing of password & acct, unattended laptop	not sharing your pwd, locking your device	securing your accounts (Google, FB, etc)
Mobile phone confiscated at protest	police	weak password, sensitive contacts on phone, access to your accounts	pseudonyms, stronger password, not bringing phone	encrypt phone

These Are Not One-off Decisions But Ongoing Choices

Formalizing these Choices Can Help us Make Better Decisions

SECURE YOUR PHONE

The best security would be to leave your phone at home.



DIGITAL SECURITY GUIDE FOR PROTESTERS

DON'T BE TRACKED

Law enforcement can intercept your SMS messages and track your location when you are protesting. With new exemptions for COVID-19 contact tracing, it's easier than ever.

Bring a **burner phone** instead of your own phone.

If you must bring your real phone, keep it in **airplane mode** and in a **signal-blocking pouch** unless you need to live stream, message for coordination, or document.

If you need to use your phone, make sure **all location services are turned off.**

If you need to message others, use **Signal, Wire,** or another encrypted messaging app. WhatsApp and iMessage are encrypted, but are owned by Facebook and Apple.

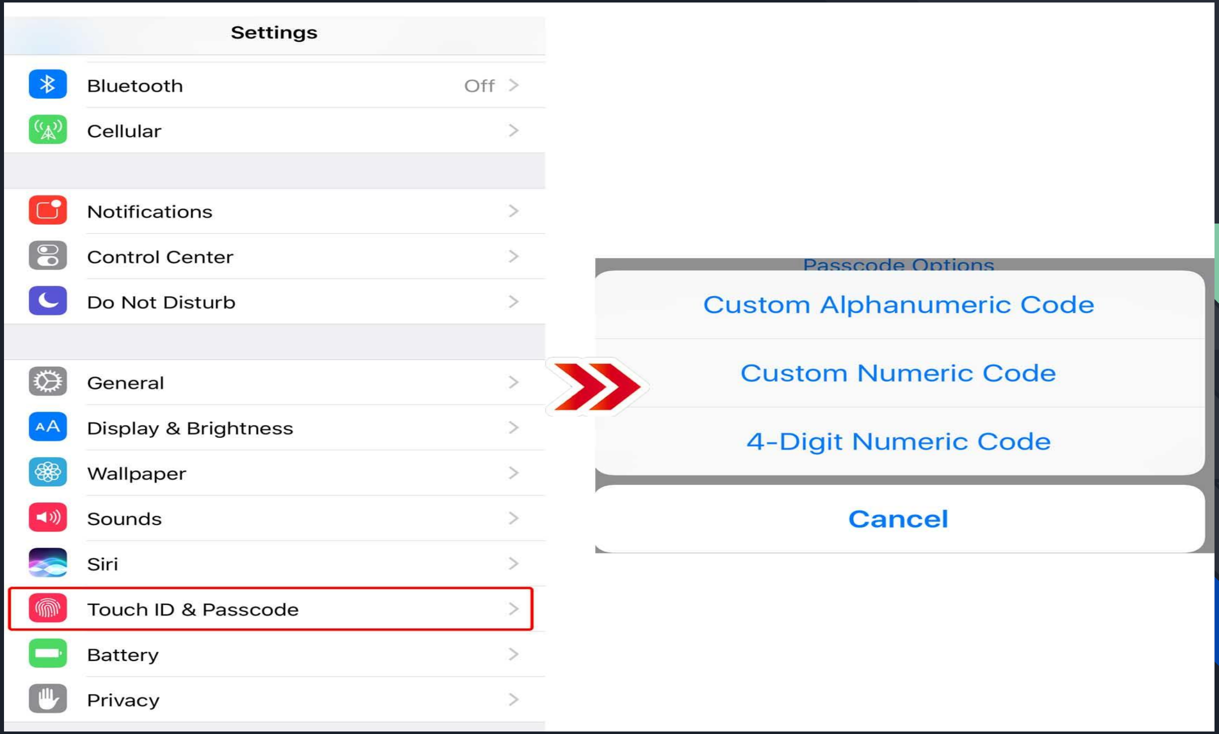
If you need to take photos, use Signal. You can automatically **blur out faces** in Signal, and you should **blur landmarks** like street signs and house numbers. Signal does not save location metadata to the photos.

Be careful sharing videos and photos online, as it can allow people shown to be identified.

But if you can't……

IPHONE

Set a Screen Lock



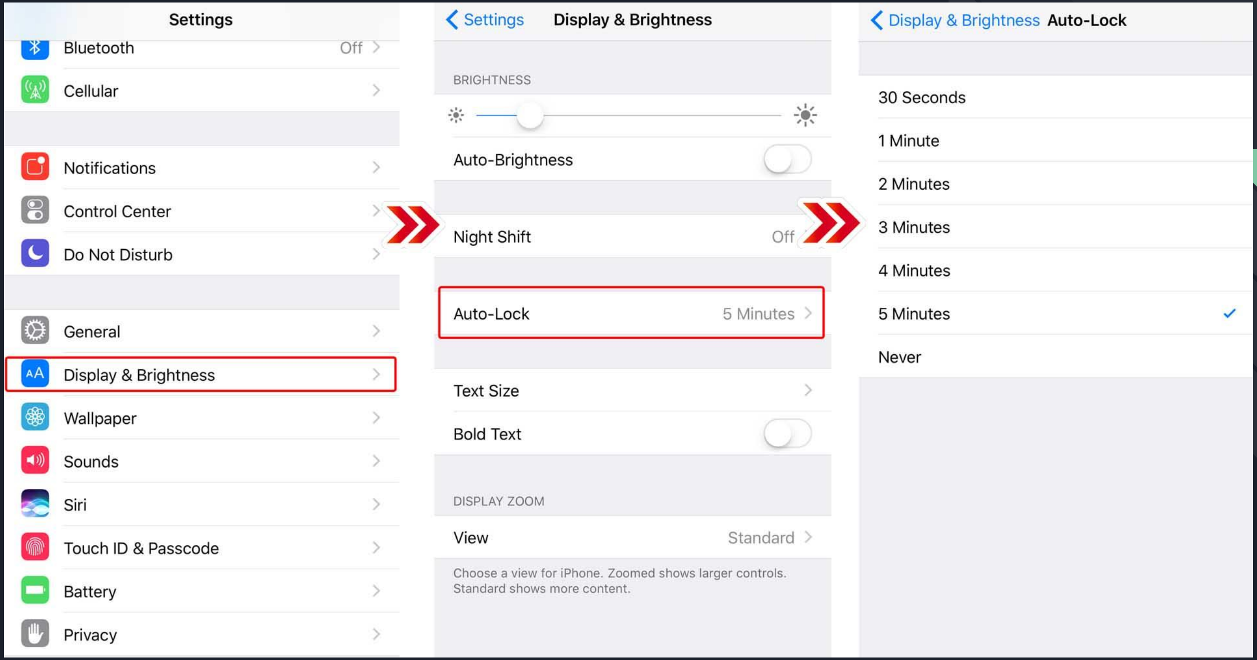
Settings

- Bluetooth — Off
- Cellular
- Notifications
- Control Center
- Do Not Disturb
- General
- Display & Brightness
- Wallpaper
- Sounds
- Siri
- Touch ID & Passcode
- Battery
- Privacy

Passcode Options

- Custom Alphanumeric Code
- Custom Numeric Code
- 4-Digit Numeric Code
- Cancel

Set Password Timer



Settings

- Bluetooth — Off
- Cellular
- Notifications
- Control Center
- Do Not Disturb
- General
- Display & Brightness
- Wallpaper
- Sounds
- Siri
- Touch ID & Passcode
- Battery
- Privacy

Settings — Display & Brightness

BRIGHTNESS

- Auto-Brightness
- Night Shift — Off
- Auto-Lock — 5 Minutes
- Text Size
- Bold Text

DISPLAY ZOOM

- View — Standard

Choose a view for iPhone. Zoomed shows larger controls. Standard shows more content.

Display & Brightness — Auto-Lock

- 30 Seconds
- 1 Minute
- 2 Minutes
- 3 Minutes
- 4 Minutes
- 5 Minutes ✓
- Never

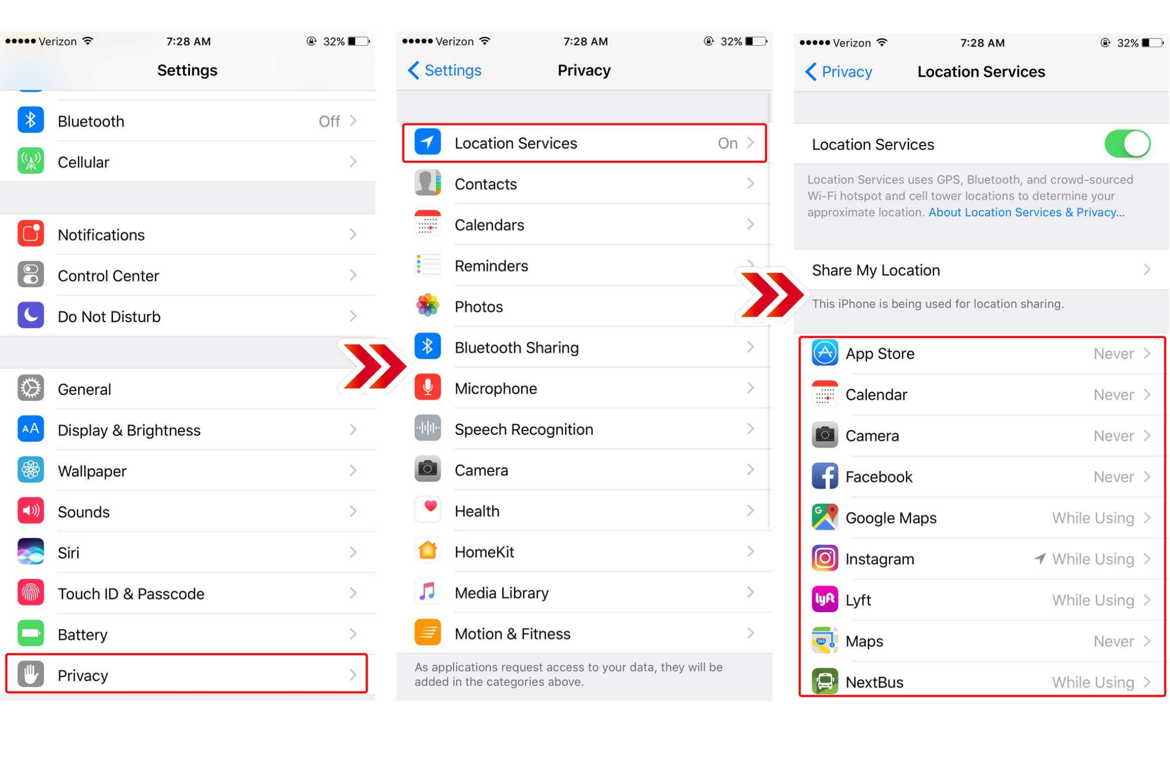
Password Strengthening

Change Passcode > Passcode Options > Custom Alphanumeric Code. Set your password/phrase.

On the bottom of the screen select the option “Erase data,” which deletes all of your phone’s contents after 10 failed password attempts.

Touch/FaceID: Press and hold the Wake button, then either one of the volume buttons simultaneously. Tap Cancel.

Turn off Location Settings



●●●●● Verizon 7:28 AM 32%

Settings

Bluetooth Off
Cellular
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
Sounds
Siri
Touch ID & Passcode
Battery
Privacy

●●●●● Verizon 7:28 AM 32%

< Settings Privacy

Location Services On
Contacts
Calendars
Reminders
Photos
Bluetooth Sharing
Microphone
Speech Recognition
Camera
Health
HomeKit
Media Library
Motion & Fitness

As applications request access to your data, they will be added in the categories above.

●●●●● Verizon 7:28 AM 32%

< Privacy Location Services

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location

This iPhone is being used for location sharing.

App Store Never
Calendar Never
Camera Never
Facebook Never
Google Maps While Using
Instagram While Using
Lyft While Using
Maps Never
NextBus While Using

Location data can be used against you. When participating in protests, remember to disable your GPS tracking.

IPHONE: Go to Settings > Privacy > Location Services. Turn off.

PixlMet

Photo Exif Metadata Viewer

http://www.pixlmetphoto.com

DuckDuckGo

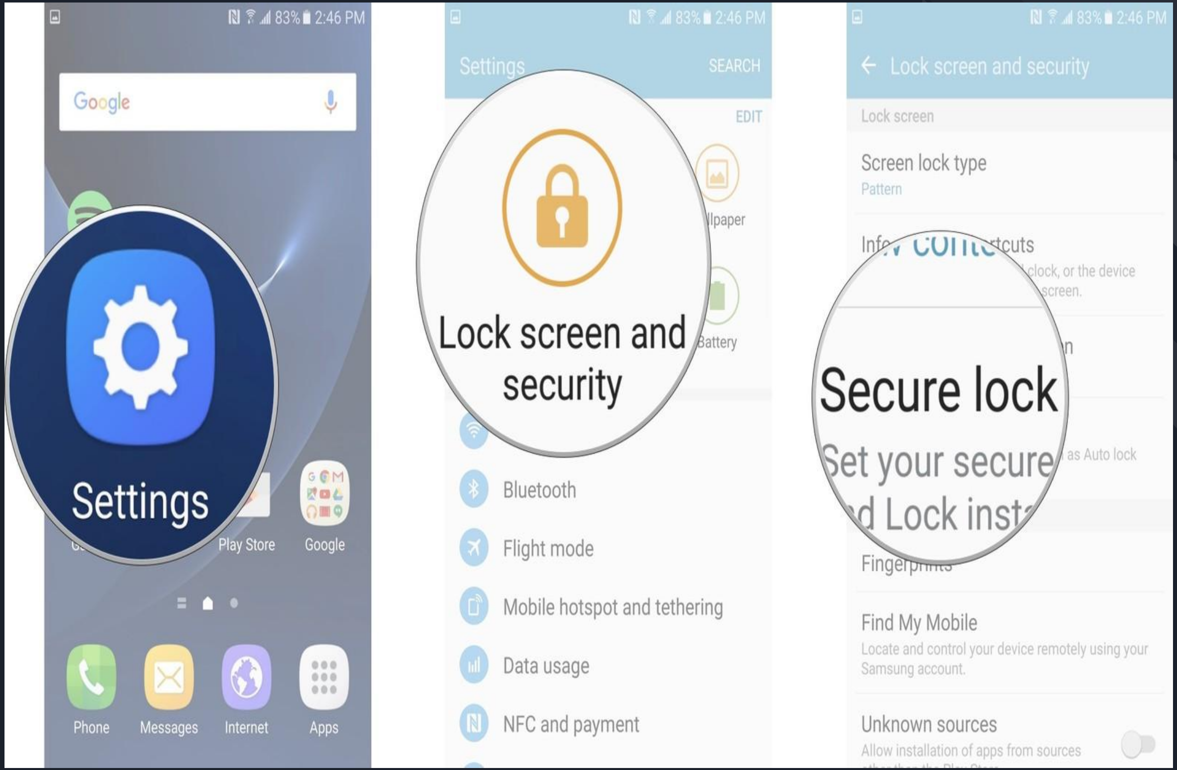
PRIVACY IS A UNIVERSAL RIGHT
MULLVAD.NET

TunnelBear

ProtonVPN
SECURE INTERNET ANYWHERE
Swiss made
ProtonVPN

ANDROID

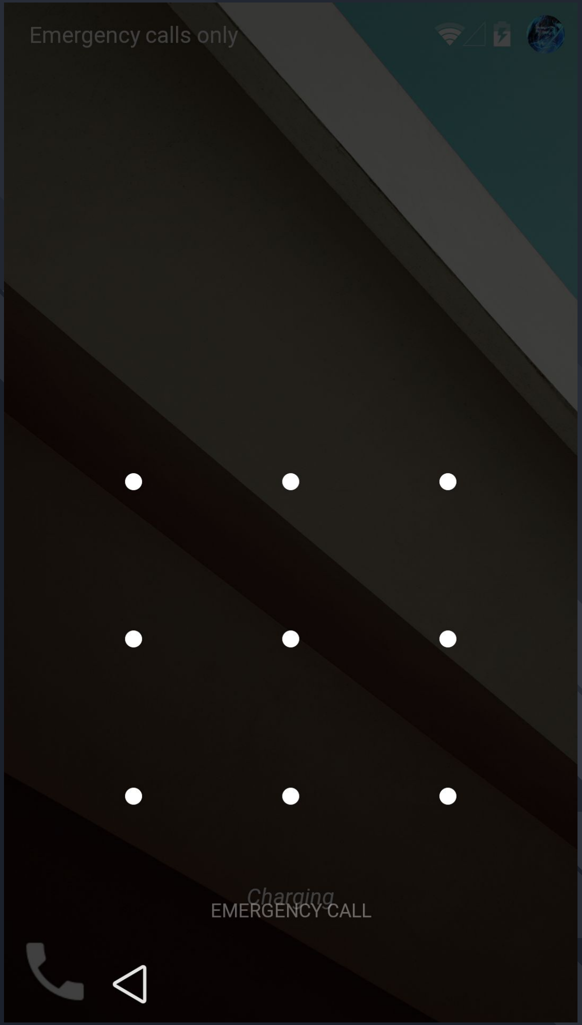
Setting up a screen lock



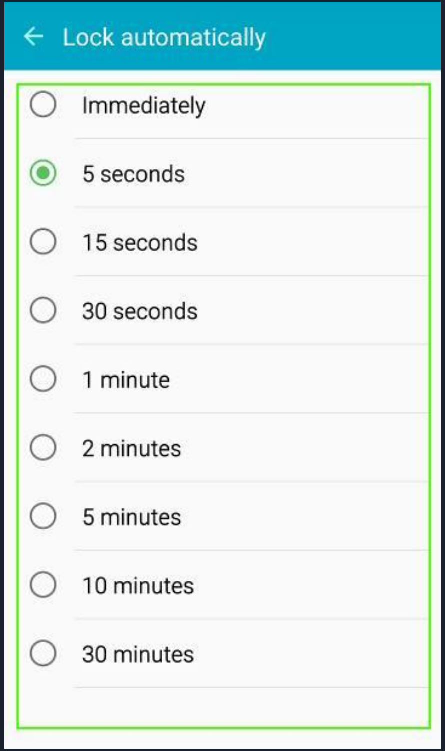
Password Strengthening

ANDROID:Go to Settings > Security > Screen Lock. Set up a password/phrase. On the same screen, select the option “encrypt device.” The quickest way to deactivate fingerprint unlock on Android devices is to simply turn them off. Once turned back on, they will require a password.

Don’t use swipe!



Security Lock Timer



← Lock automatically

○ Immediately

● 5 seconds

○ 15 seconds

○ 30 seconds

○ 1 minute

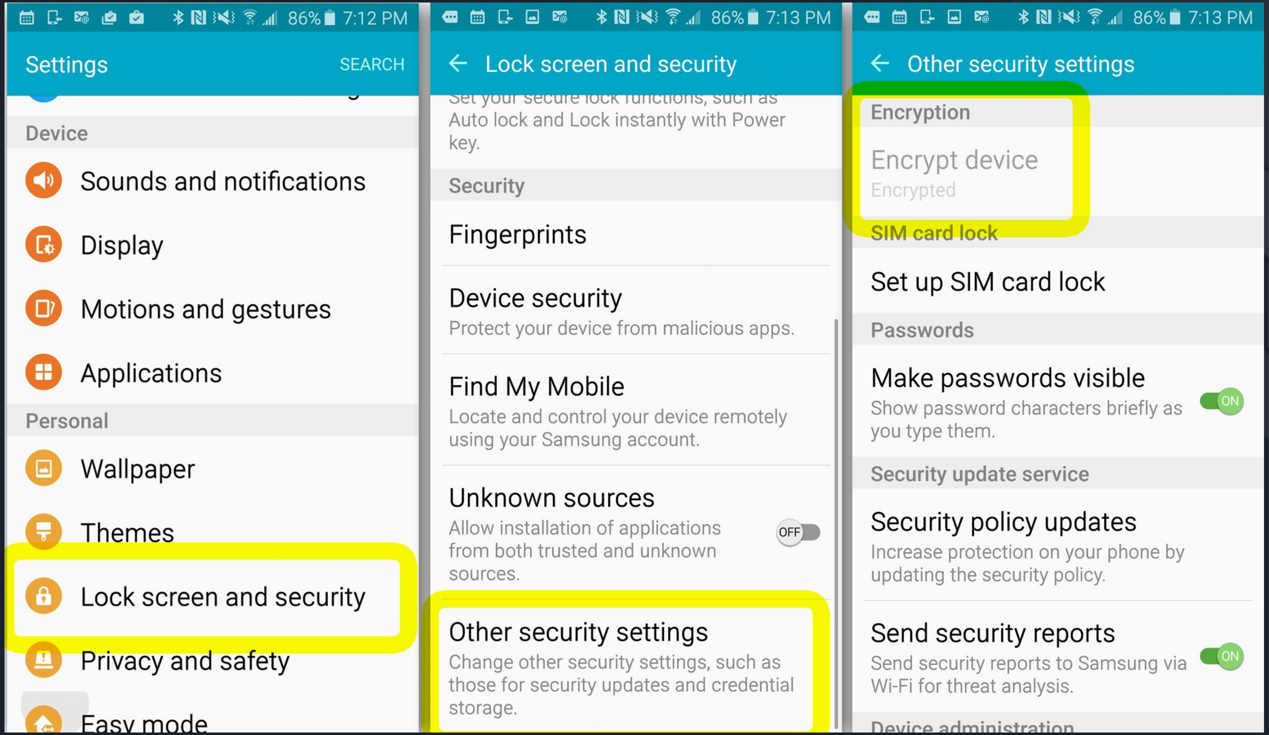
○ 2 minutes

○ 5 minutes

○ 10 minutes

○ 30 minutes

Android Disk Encryption



86% 7:12 PM

Settings SEARCH

Device

Sounds and notifications

Display

Motions and gestures

Applications

Personal

Wallpaper

Themes

Lock screen and security

Privacy and safety

Easy mode

86% 7:13 PM

← Lock screen and security

Set your secure lock functions, such as Auto lock and Lock instantly with Power key.

Security

Fingerprints

Device security

Protect your device from malicious apps.

Find My Mobile

Locate and control your device remotely using your Samsung account.

Unknown sources

Allow installation of applications from both trusted and unknown sources.

OFF

Other security settings

Change other security settings, such as those for security updates and credential storage.

86% 7:13 PM

← Other security settings

Encryption

Encrypt device

Encrypted

SIM card lock

Set up SIM card lock

Passwords

Make passwords visible

Show password characters briefly as you type them.

ON

Security update service

Security policy updates

Increase protection on your phone by updating the security policy.

Send security reports

Send security reports to Samsung via Wi-Fi for threat analysis.

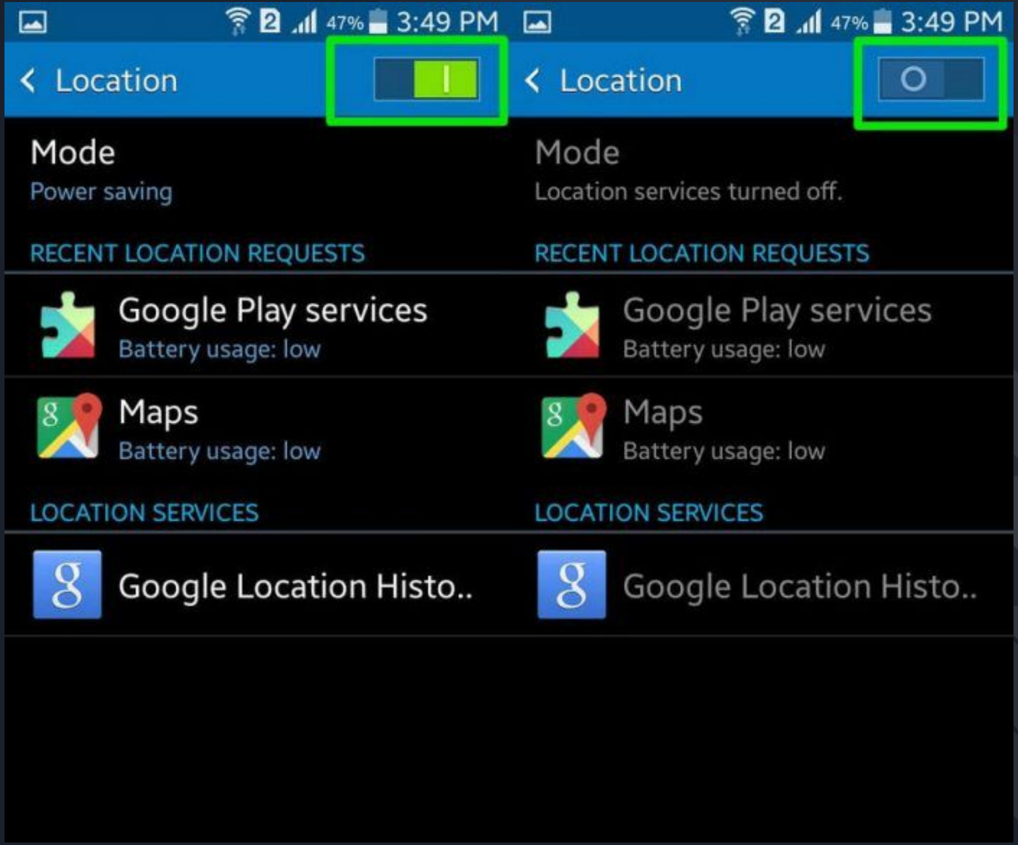
ON

Device administration

Deactivating Location Services

Location data can be used against you. When participating in protests, remember to disable your GPS tracking.

Android: Look for the Privacy subhead > Location. Turn off “Use location.”



47% 3:49 PM

Location

Mode

Power saving

RECENT LOCATION REQUESTS

Google Play services

Battery usage: low

Maps

Battery usage: low

LOCATION SERVICES

Google Location Histo..

47% 3:49 PM

Location

Mode

Location services turned off.

RECENT LOCATION REQUESTS

Google Play services

Battery usage: low

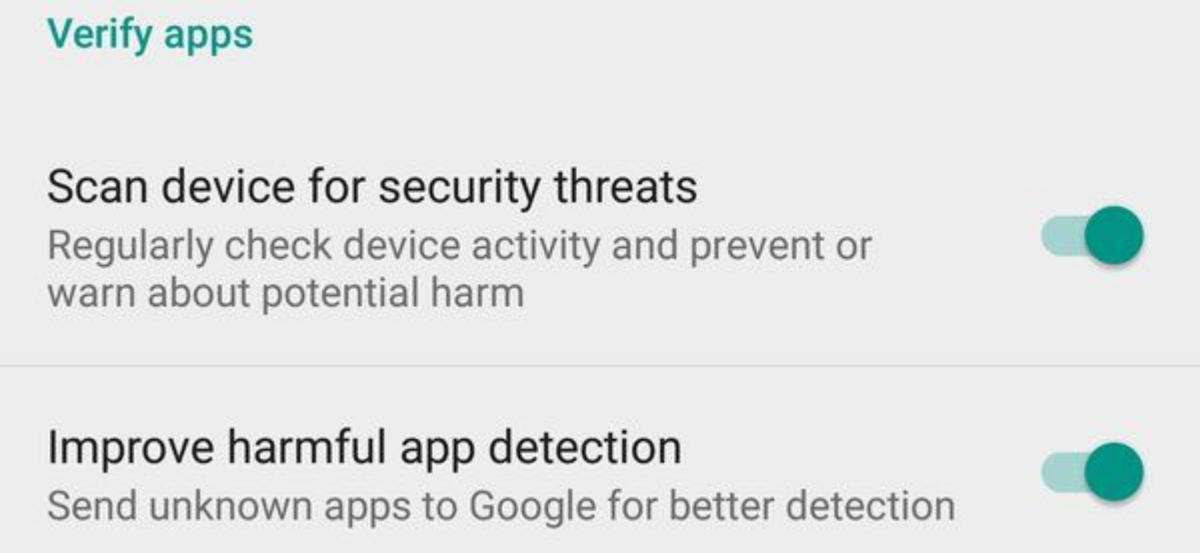
Maps

Battery usage: low

LOCATION SERVICES

Google Location Histo..

Google Services Verify App to prevent Malware

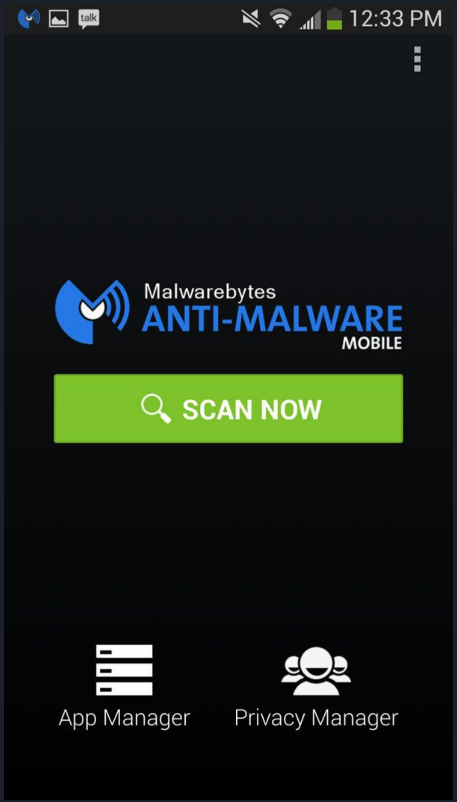


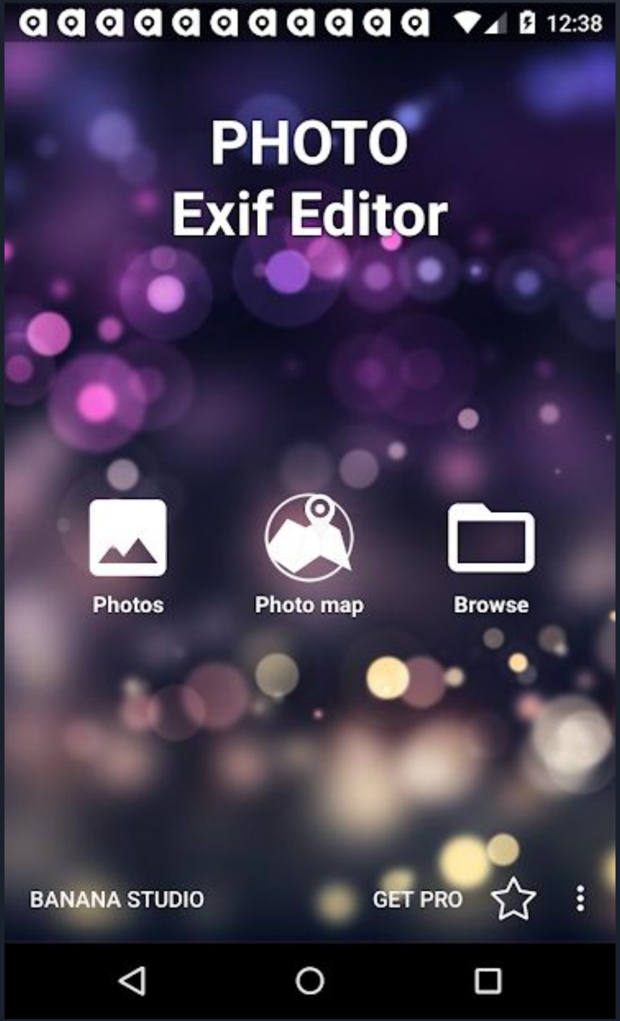
Verify apps

Scan device for security threats
Regularly check device activity and prevent or warn about potential harm
●

Improve harmful app detection
Send unknown apps to Google for better detection
●

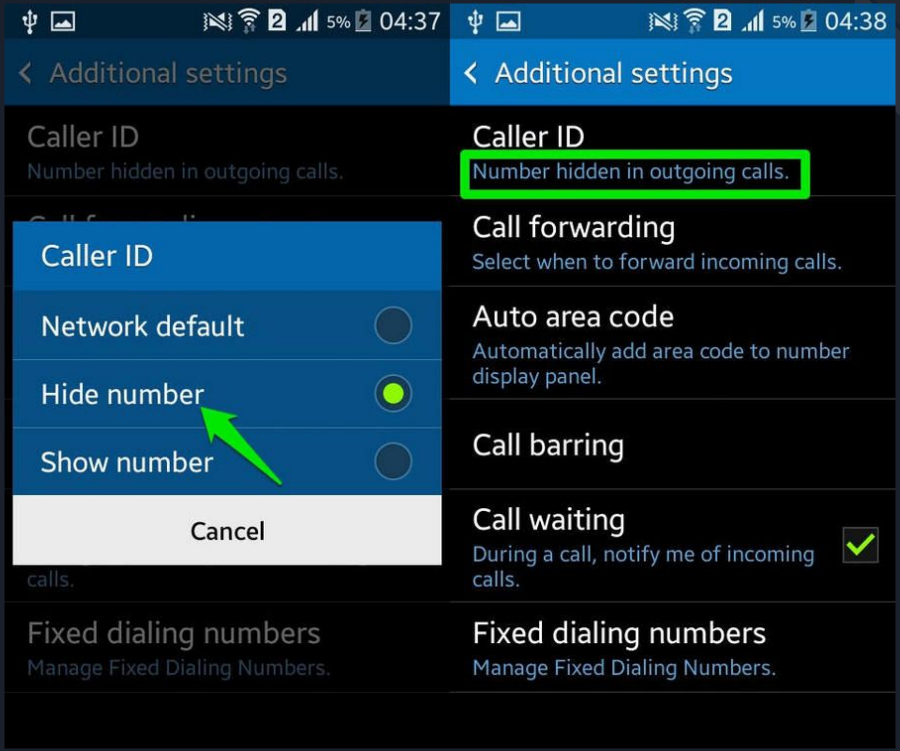
Install Malwarebytes for Android




12:38
PHOTO
Exif Editor
Photos
Photo map
Browse
BANANA STUDIO
GET PRO

Set the security lock timer, which will automatically lock your phone after a specified time.

Hide your Caller ID



5% 04:37

Additional settings

Caller ID
Number hidden in outgoing calls.

Caller ID

Network default ○

Hide number ●

Show number ○

Cancel

calls.

Fixed dialing numbers
Manage Fixed Dialing Numbers.

5% 04:38

Additional settings

Caller ID
Number hidden in outgoing calls.

Call forwarding
Select when to forward incoming calls.

Auto area code
Automatically add area code to number display panel.

Call barring

Call waiting ☑
During a call, notify me of incoming calls.

Fixed dialing numbers
Manage Fixed Dialing Numbers.

Update your phone operating system:
Go to: settings -> About phone -> updates -> check for updates.

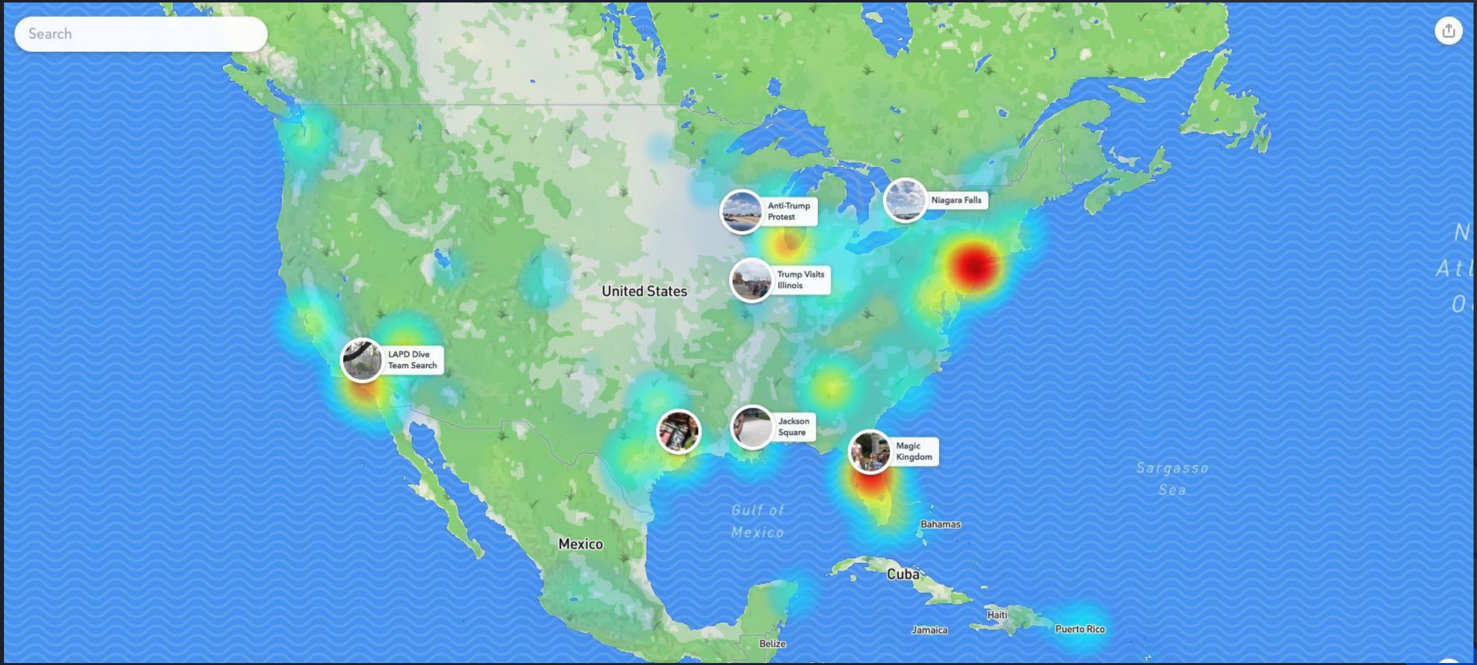
SECURE YOUR APPS

Popular apps we will cover:

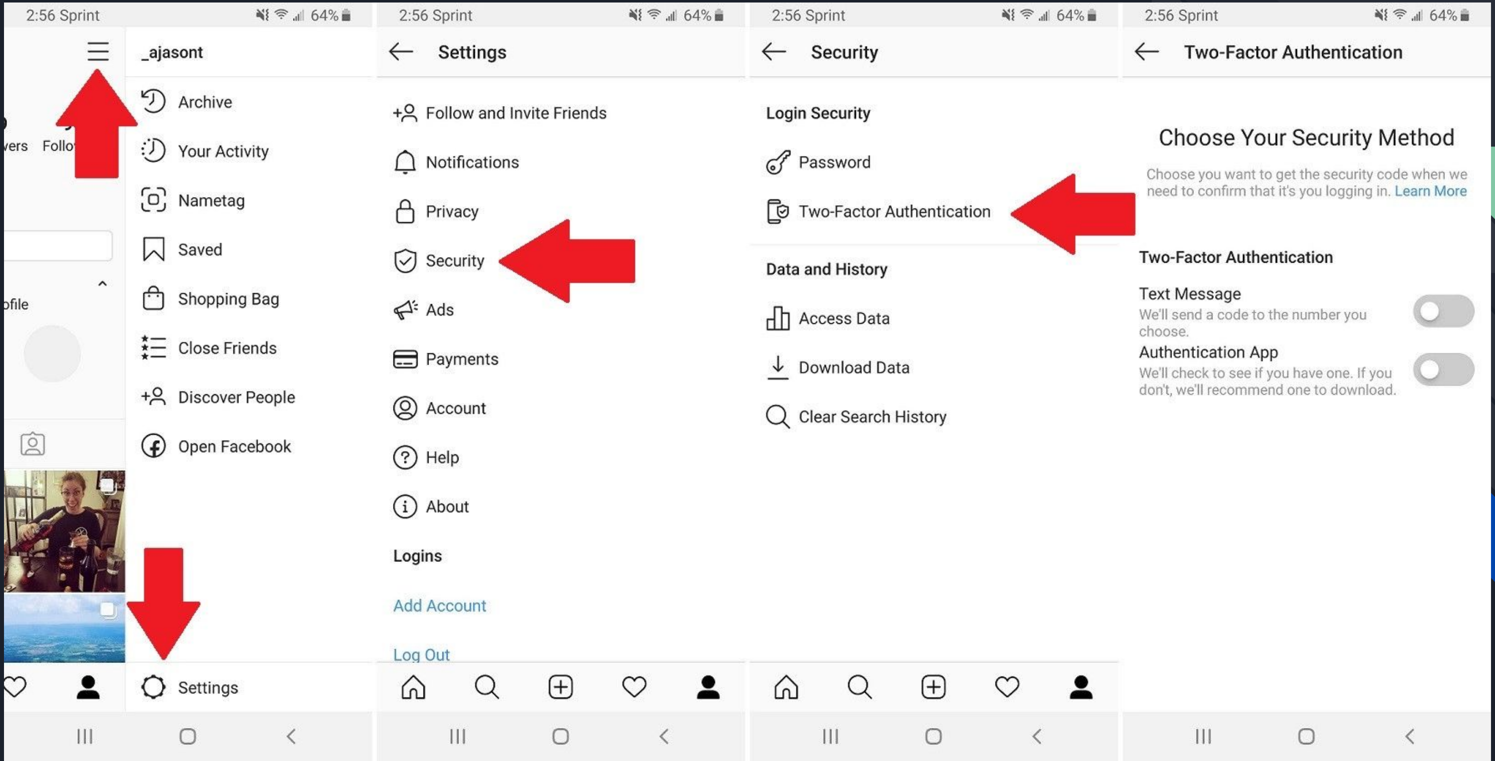
Snapchat
Instagram
TikTok

The more apps you have on your device the more attack vectors a bad actor has to exploit.
Limiting the amount of apps on your device keeps it more secure.
Haven’t used an app in three months? Delete it.

Snapchat


Search
Anti-Trump Protest
Niagara Falls
Trump Visits Illinois
United States
LAPD Dive Team Search
Jackson Square
Magic Kingdom
N
Atl
O
Sargasso Sea
Gulf of Mexico
Bahamas
Mexico
Cuba
Haiti
Jamaica
Puerto Rico
Belize

Instagram



2:56 Sprint 64%

_ajasont

- Archive
- Your Activity
- Nametag
- Saved
- Shopping Bag
- Close Friends
- Discover People
- Open Facebook
- Settings

2:56 Sprint 64%

Settings

- Follow and Invite Friends
- Notifications
- Privacy
- Security
- Ads
- Payments
- Account
- Help
- About

Logins

Add Account

Log Out

2:56 Sprint 64%

Security

Login Security

- Password
- Two-Factor Authentication

Data and History

- Access Data
- Download Data
- Clear Search History

2:56 Sprint 64%

Two-Factor Authentication

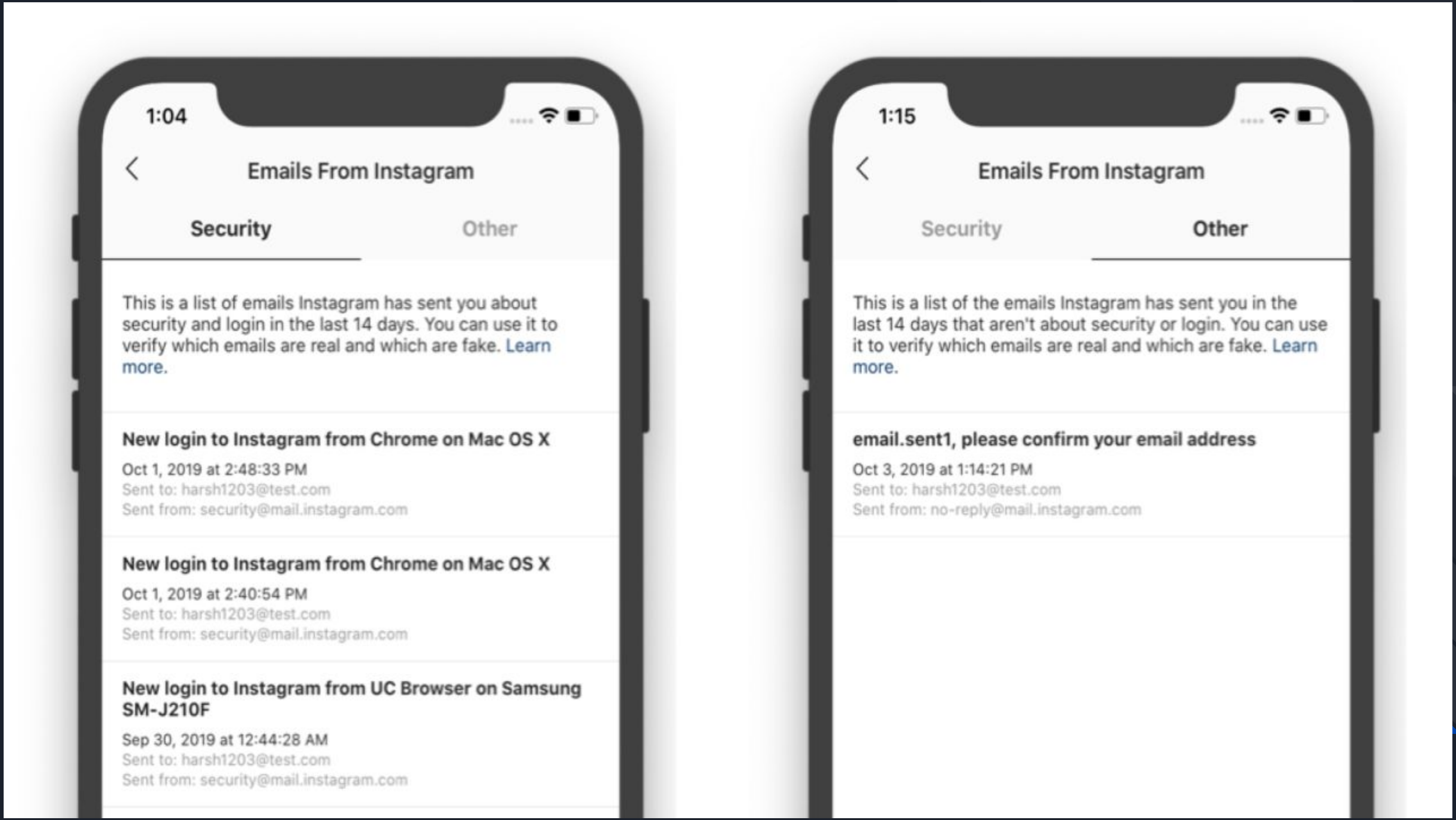
Choose Your Security Method

Choose you want to get the security code when we need to confirm that it's you logging in. Learn More

Two-Factor Authentication

Text Message ○
We'll send a code to the number you choose.

Authentication App ○
We'll check to see if you have one. If you don't, we'll recommend one to download.



Emails From Instagram

This is a list of emails Instagram has sent you about security and login in the last 14 days. You can use it to verify which emails are real and which are fake. Learn more.

New login to Instagram from Chrome on Mac OS X

Oct 1, 2019 at 2:48:33 PM
Sent to: harsh1203@test.com
Sent from: security@mail.instagram.com

New login to Instagram from Chrome on Mac OS X

Oct 1, 2019 at 2:40:54 PM
Sent to: harsh1203@test.com
Sent from: security@mail.instagram.com

New login to Instagram from UC Browser on Samsung SM-J210F

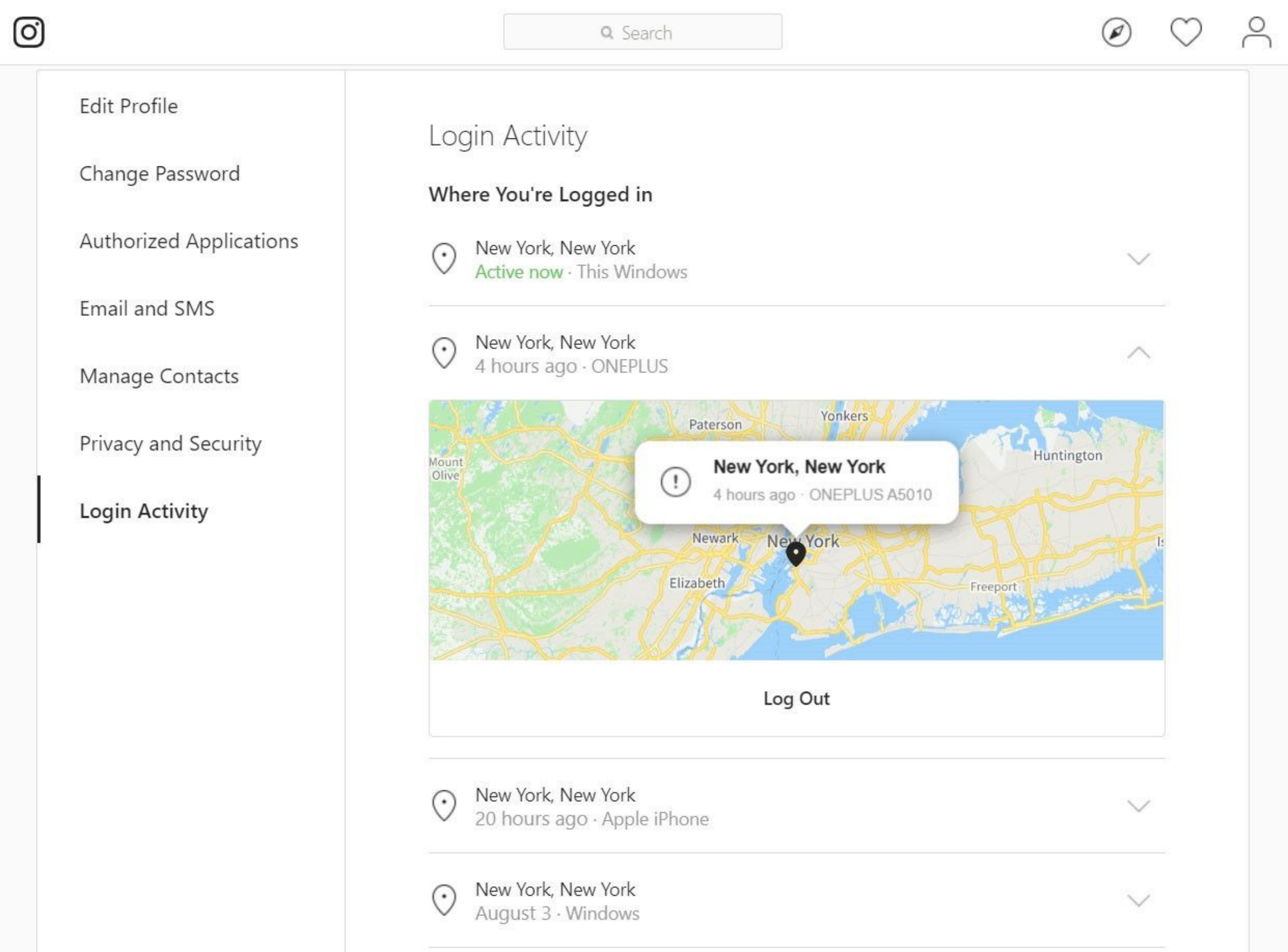
Sep 30, 2019 at 12:44:28 AM
Sent to: harsh1203@test.com
Sent from: security@mail.instagram.com

Emails From Instagram

This is a list of the emails Instagram has sent you in the last 14 days that aren't about security or login. You can use it to verify which emails are real and which are fake. Learn more.

email.sent1, please confirm your email address

Oct 3, 2019 at 1:14:21 PM
Sent to: harsh1203@test.com
Sent from: no-reply@mail.instagram.com



Login Activity

Where You're Logged in

New York, New York
Active now · This Windows

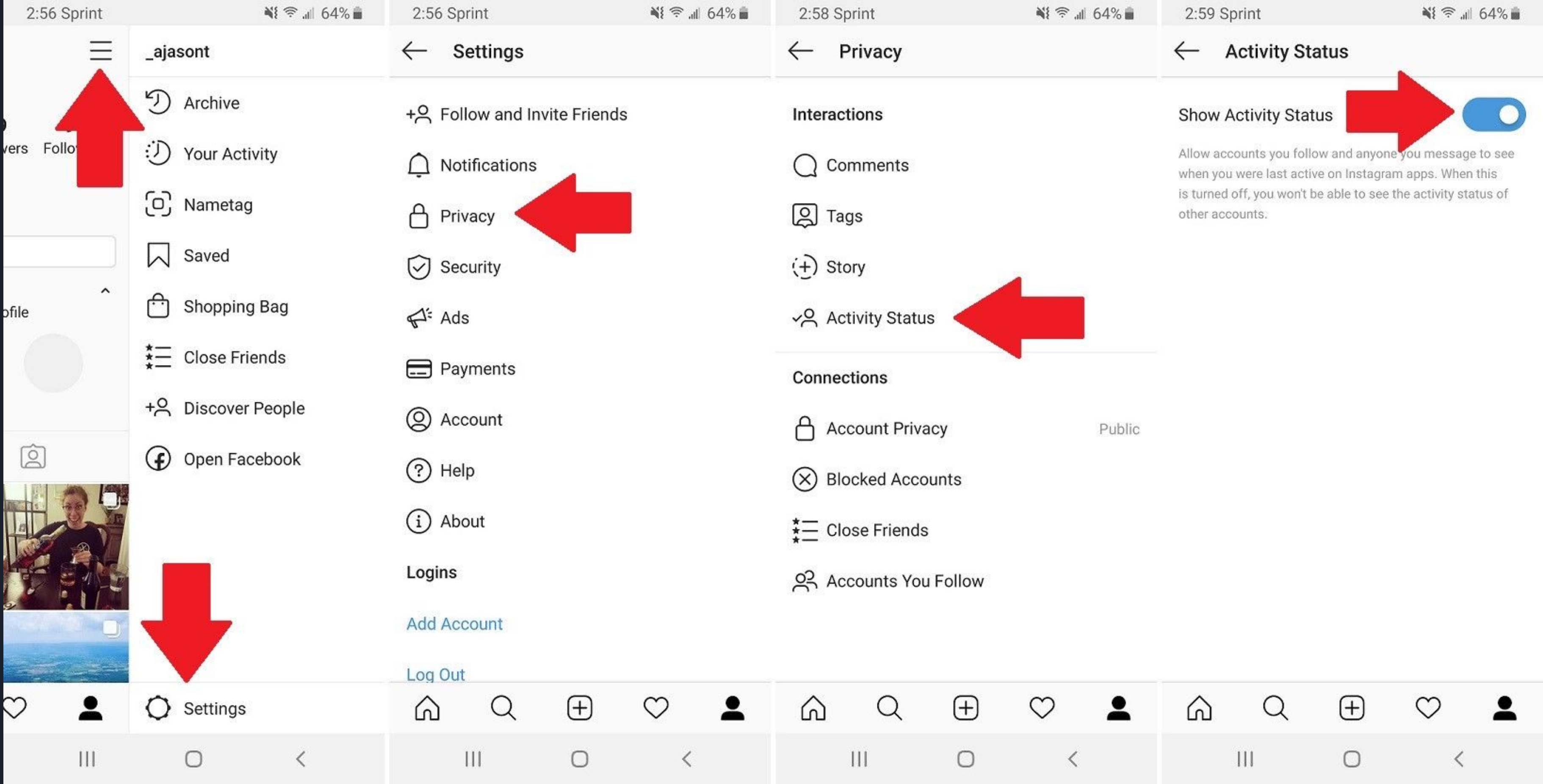
New York, New York
4 hours ago · ONEPLUS

New York, New York
4 hours ago · ONEPLUS A5010

Log Out

New York, New York
20 hours ago · Apple iPhone

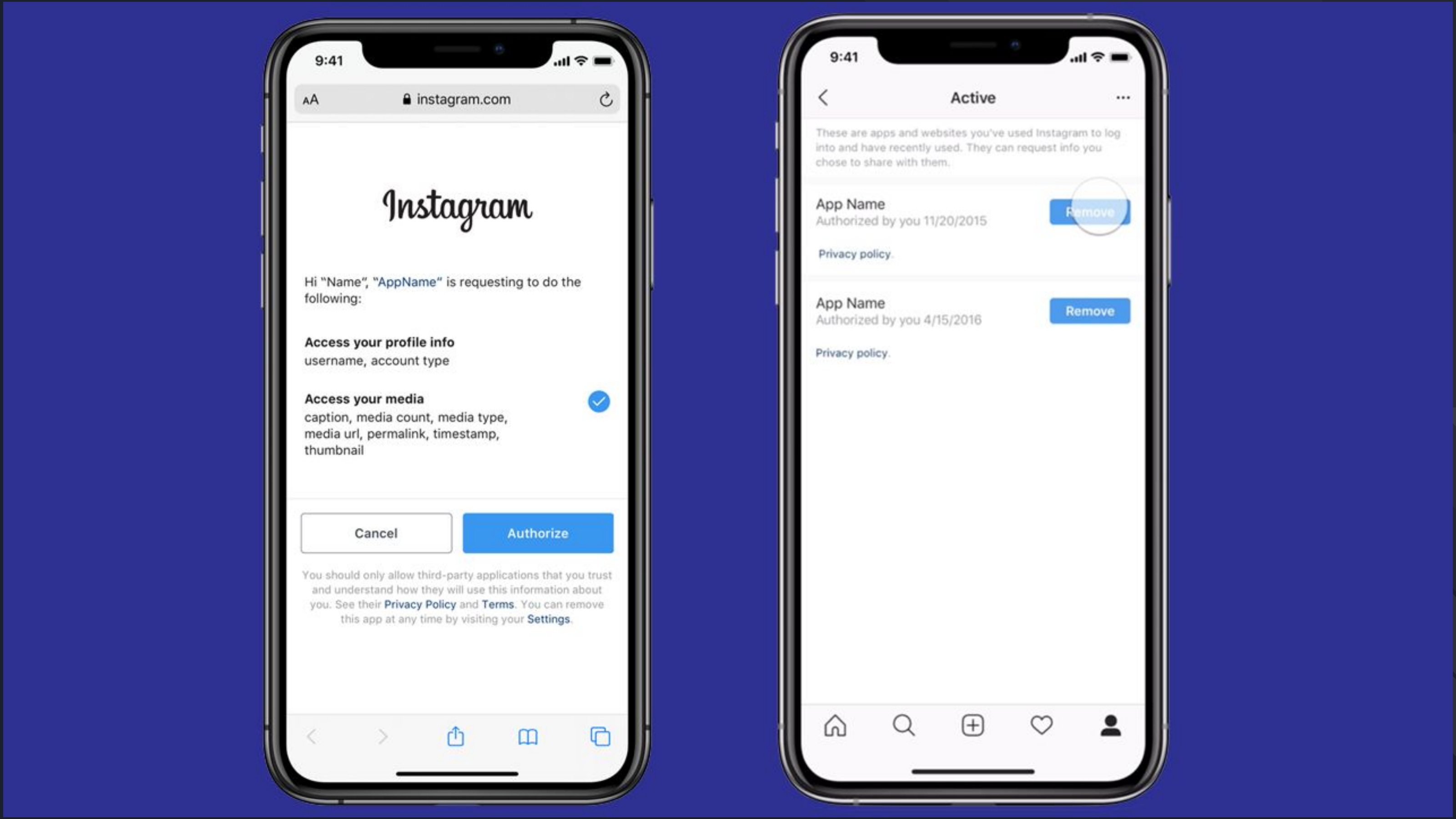
New York, New York
August 3 · Windows



Show Activity Status ●

Allow accounts you follow and anyone you message to see when you were last active on Instagram apps. When this is turned off, you won't be able to see the activity status of other accounts.

Revoke 3rd Party Access



9:41

AA instagram.com

Instagram

Hi "Name", "AppName" is requesting to do the following:

Access your profile info
username, account type

Access your media ✓
caption, media count, media type, media url, permalink, timestamp, thumbnail

Cancel | Authorize

You should only allow third-party applications that you trust and understand how they will use this information about you. See their Privacy Policy and Terms. You can remove this app at any time by visiting your Settings.

9:41

Active

These are apps and websites you've used Instagram to log into and have recently used. They can request info you chose to share with them.

App Name
Authorized by you 11/20/2015 — Remove
Privacy policy

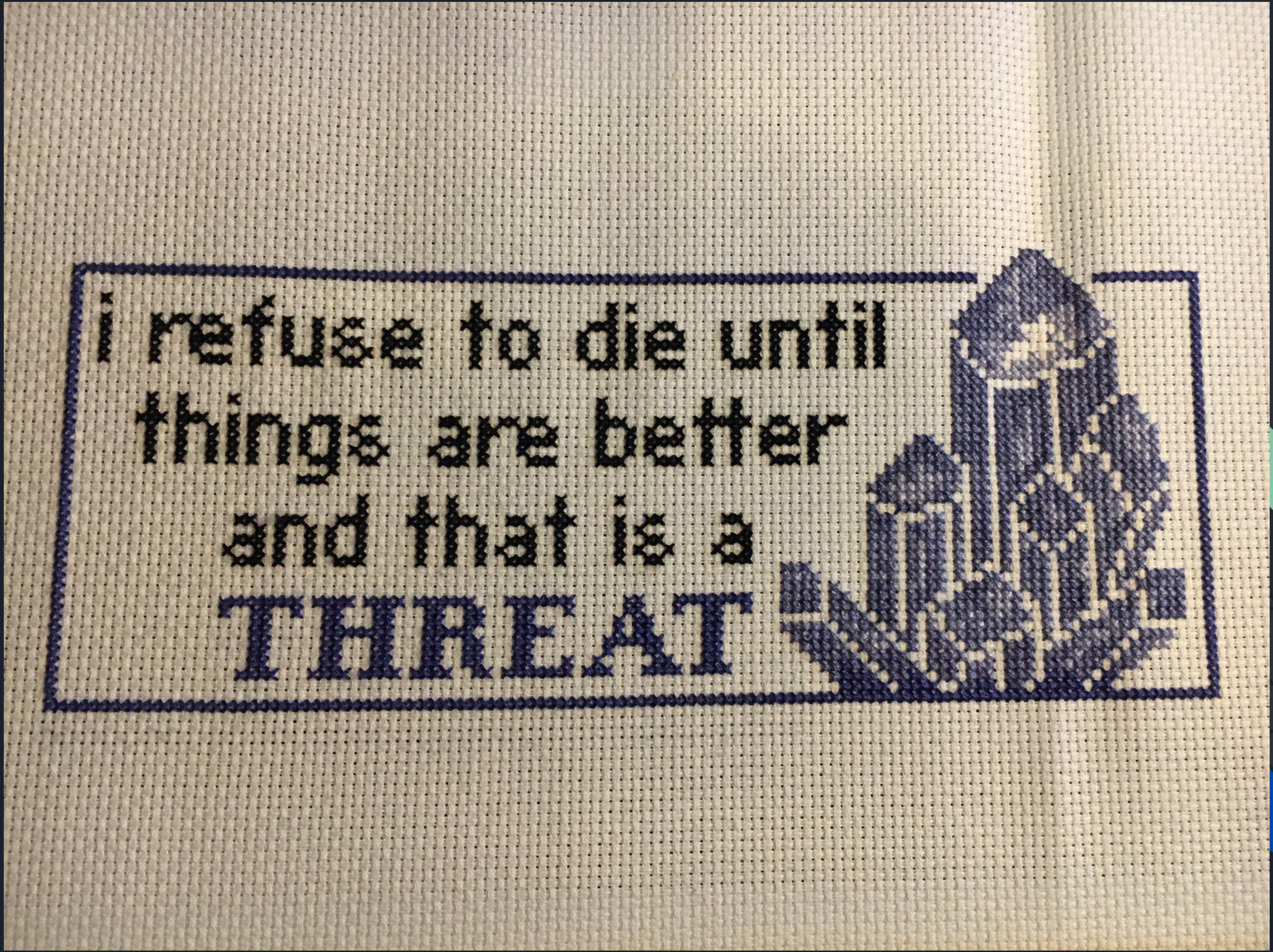
App Name
Authorized by you 4/15/2016 — Remove
Privacy policy

TikTok

DELETE THE ENTIRE APP DO NOT USE IT

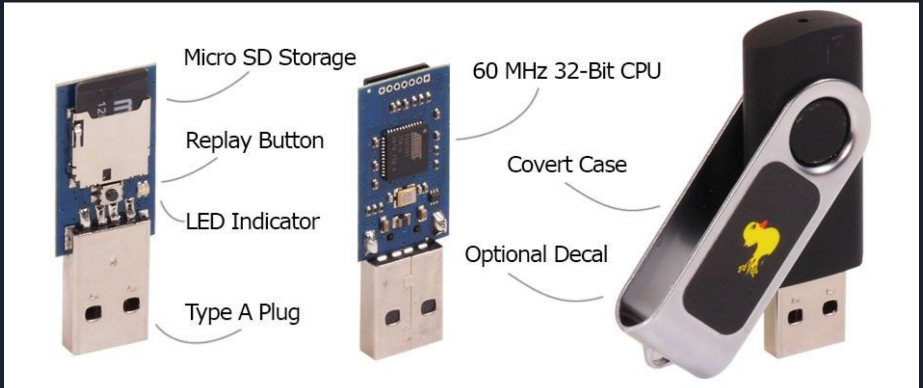
Preparing Social Media for Your Death……..

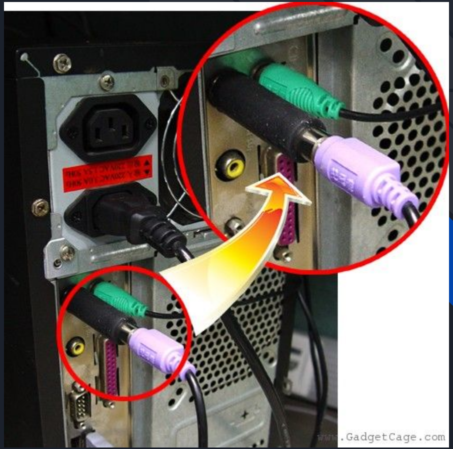
https://www.pcmag.com/how-to/how-to-prepare-your-digital-life-for-your-death


i refuse to die until
things are better
and that is a
THREAT

SECURE YOUR COMPUTER

Physical Attack Vectors





Digital Attack Vectors

RATs (Remote Access Tools)

Malicious docs disguised .exe

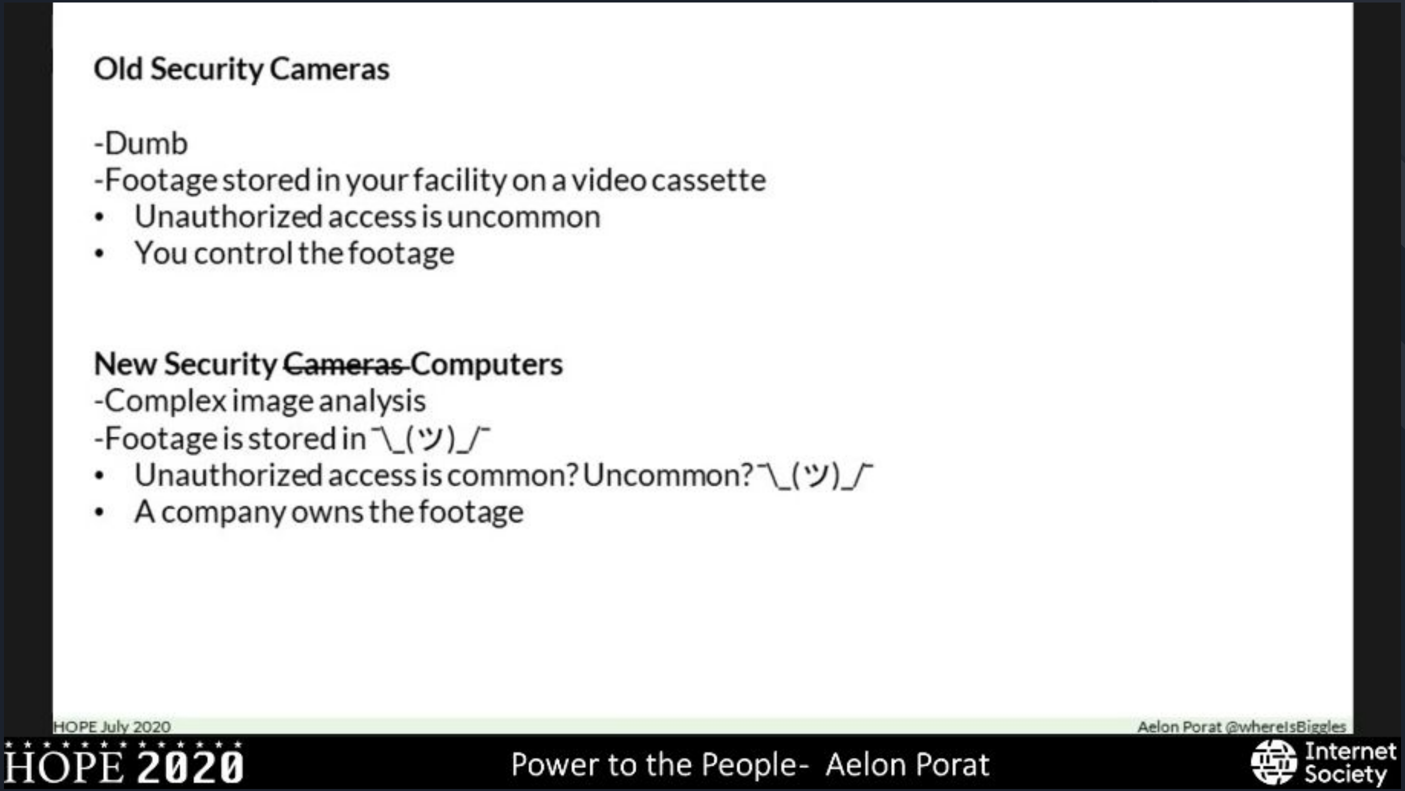
App Permission (granting cell phone camera permission allows access foreverrrrr)

Location data (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html) Cell phone carriers sell your data so do cops

Facial sentiment recognition

Data Breaches (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

Security Camera



Old Security Cameras

-Dumb
-Footage stored in your facility on a video cassette

- Unauthorized access is uncommon
- You control the footage

New Security ~~Cameras~~ Computers
-Complex image analysis
-Footage is stored in ¯_(ツ)_/¯

- Unauthorized access is common? Uncommon? ¯_(ツ)_/¯
- A company owns the footage

HOPE July 2020

Aelon Porat @whereIsBiggles

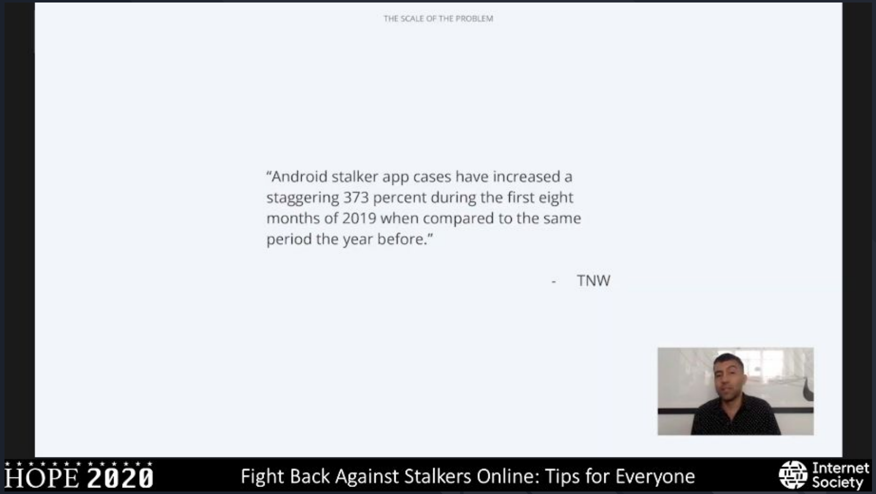
HOPE 2020

Power to the People- Aelon Porat

Internet Society

Computer/Phone Tracking and Stalkerware

iCloud is one of the largest targets
Google Maps is also commonly used
Apples FindMyPhone App
Email is also an unexpected route for stalkerware
Gaining access to any of these will pwn the device

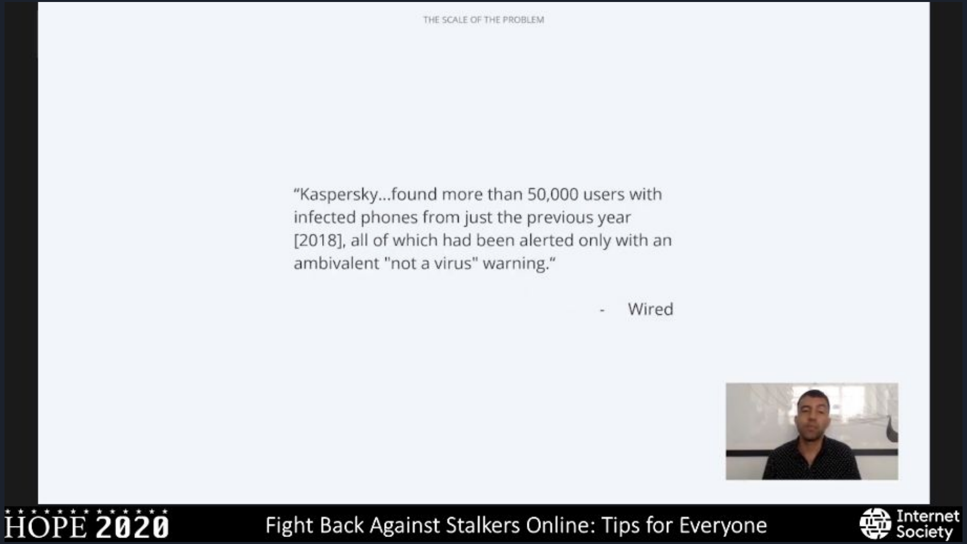


THE SCALE OF THE PROBLEM

"Android stalker app cases have increased a staggering 373 percent during the first eight months of 2019 when compared to the same period the year before."

- TNW

HOPE 2020 Fight Back Against Stalkers Online: Tips for Everyone Internet Society



THE SCALE OF THE PROBLEM

"Kaspersky...found more than 50,000 users with infected phones from just the previous year [2018], all of which had been alerted only with an ambivalent "not a virus" warning."

- Wired

HOPE 2020 Fight Back Against Stalkers Online: Tips for Everyone Internet Society

Stalkerware

Dual use apps:
Anti-theft Apps like Cerberus

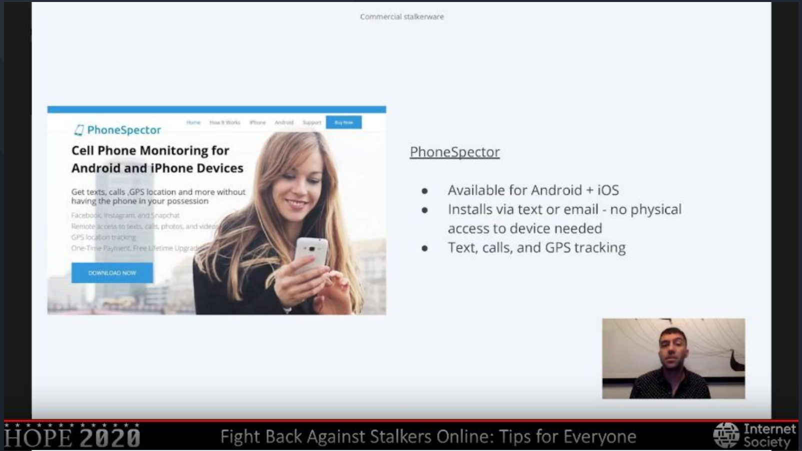
State Sponsored Stalkerware:
Absher developed by Saudi Gov

Commercial Stalkerware
PhoneSpector
FlexiSpy
SpyPhone Android Plus

Unknown State Apps

Root'd or Jailbreaking

Gifted Devices



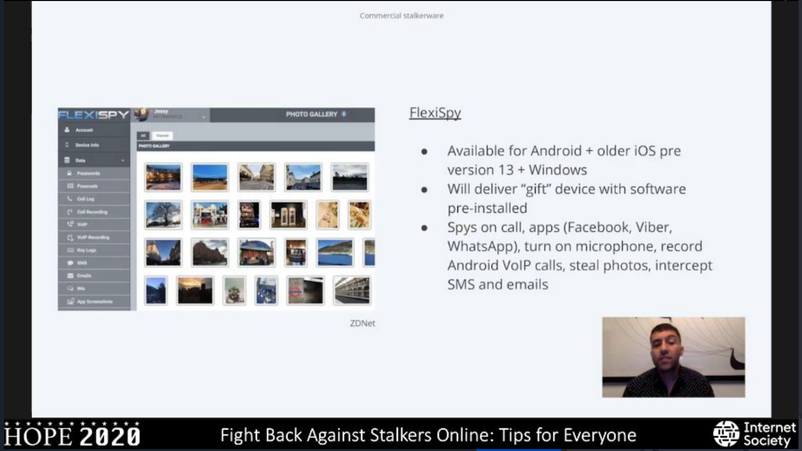
Commercial stalkerware

PhoneSpector
Home
How It Works
iPhone
Android
Support
Buy Now
Cell Phone Monitoring for Android and iPhone Devices
Get texts, calls ,GPS location and more without having the phone in your possession
Facebook, Instagram, and Snapchat
Remote access to texts, calls, photos, and videos
GPS location tracking
One-Time Payment, Free Lifetime Upgrades
DOWNLOAD NOW

PhoneSpector

- Available for Android + iOS
- Installs via text or email - no physical access to device needed
- Text, calls, and GPS tracking

HOPE 2020 Fight Back Against Stalkers Online: Tips for Everyone Internet Society



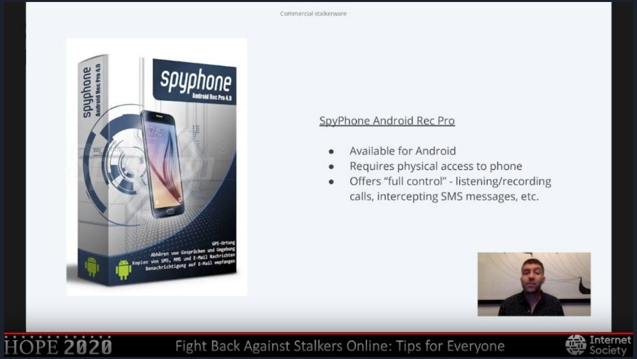
Commercial stalkerware

ZDNet

FlexiSpy

- Available for Android + older iOS pre version 13 + Windows
- Will deliver "gift" device with software pre-installed
- Spys on call, apps (Facebook, Viber, WhatsApp), turn on microphone, record Android VoIP calls, steal photos, intercept SMS and emails

HOPE 2020 Fight Back Against Stalkers Online: Tips for Everyone Internet Society



Commercial stalkerware

spyphone
Android Rec Pro 4.0
GPS-Ortung
Abhören von Gesprächen und Umgebung
Kopien von SMS, MMS und E-Mail Nachrichten
Benachrichtigung auf E-Mail empfangen

SpyPhone Android Rec Pro

- Available for Android
- Requires physical access to phone
- Offers "full control" - listening/recording calls, intercepting SMS messages, etc.

HOPE 2020 Fight Back Against Stalkers Online: Tips for Everyone Internet Society

Protecting Yourself from Stalkerware

Malwarebytes

Restart your phone back to factory setting, erasing everything on the phone.

iPhone > Android

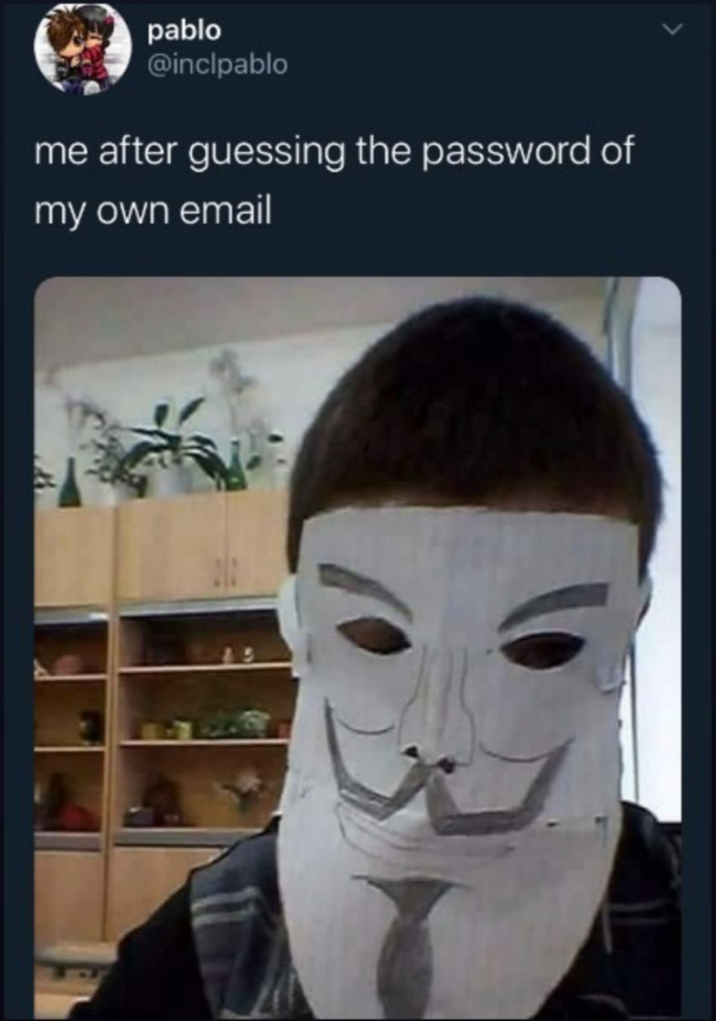
2FA on everything!

Don’t reuse passwords!

Backup Devices

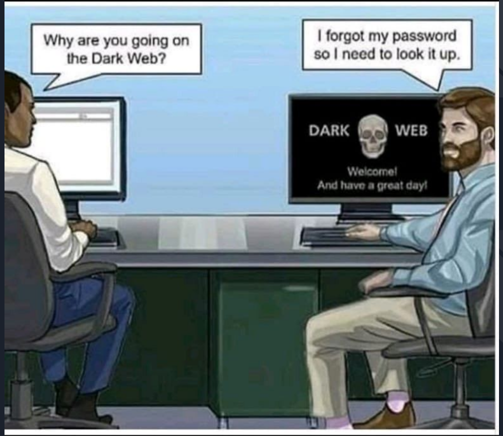
Be aware of warning signs of compromised devices:
Battery drain larger than usual.
Spike in data usage.
Trouble turning phone off.

CREATE A GOOD PASSPHRASE



pablo
@inclpablo

me after guessing the password of my own email


Why are you going on the Dark Web?
I forgot my password so I need to look it up.
DARK WEB
Welcome! And have a great day!

YOUR PASSWORD IS TOO WEAK.
WHO'S WEAK NOW?
WARANDPEAS.COM

~~PASSWORD!~~

PASSPHRASE!

DiceWare!

KEYS TO A GOOD PASSPHRASE

KEEP IT LONG

KEEP IT COMPLEX

KEEP IT PRACTICAL

KEEP IT FRESH

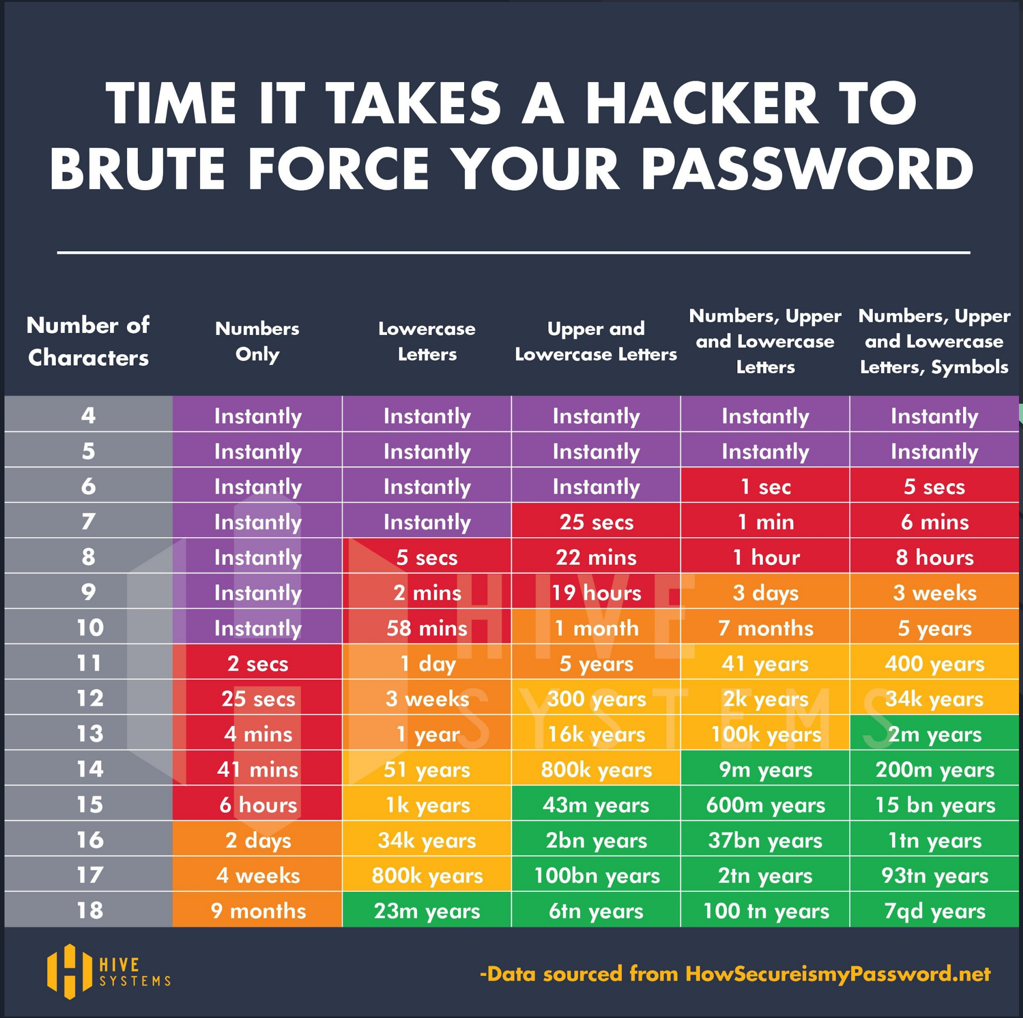
NO PERSONAL DETAILS

AND DON’T EVER EVER EVER SHARE

Test password strength:

https://howsecureismypassword.net

Do NOT enter your real password



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

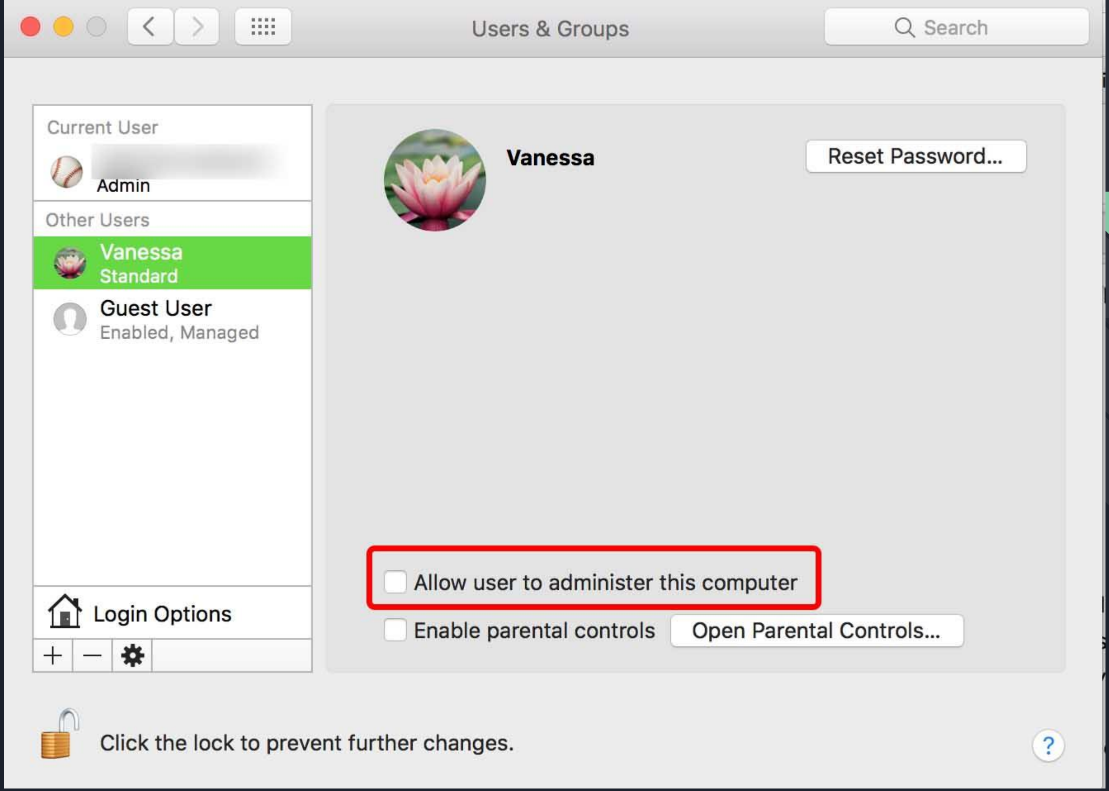
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

ENABLE MULTIPLE USERS

New accounts for mac



☐ Allow user to administer this computer

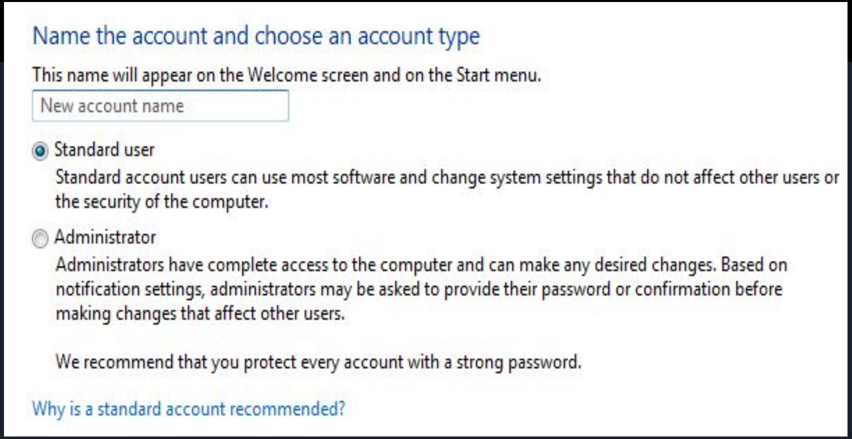
☐ Enable parental controls

Click the lock to prevent further changes.

New Accounts for Windows

To create a new account on Windows 10, **Start** > **Settings** > **Accounts** > **Family & other people** > **Add someone else to this PC**

To create a new account on previous versions click **Start > Control Panel** >**User Accounts and Family Safety** > **User Accounts** > **Manage another account** > **Create a new account**.



Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

New account name

● Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

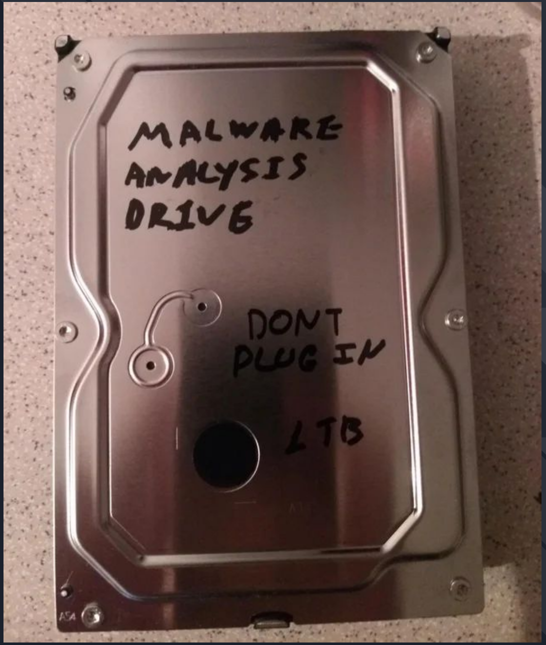
○ Administrator

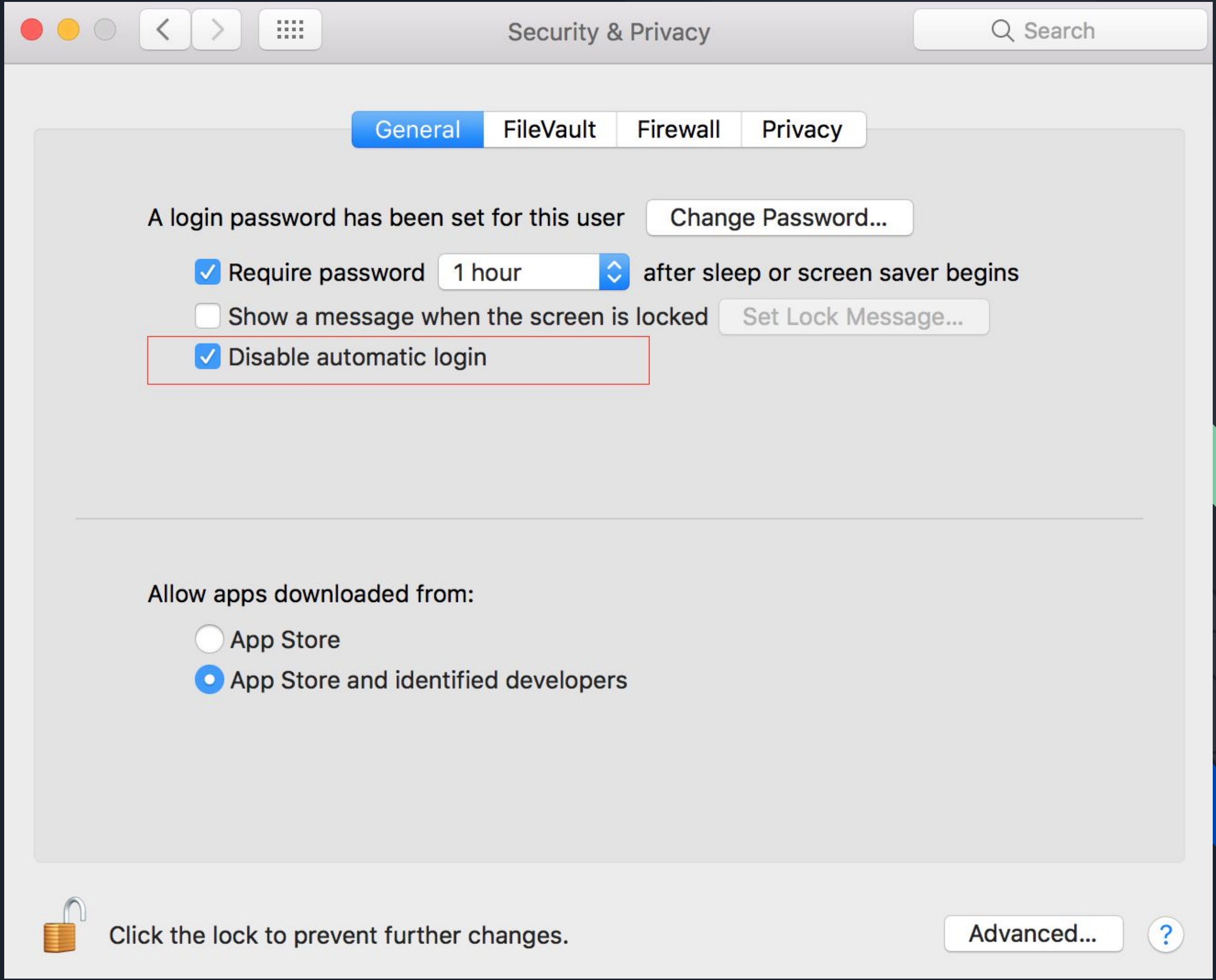
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

Why is a standard account recommended?

ENABLE FULL DISK ENCRYPTION





A login password has been set for this user [Change Password...]

☑ Require password [1 hour] after sleep or screen saver begins

□ Show a message when the screen is locked [Set Lock Message...]

☑ Disable automatic login

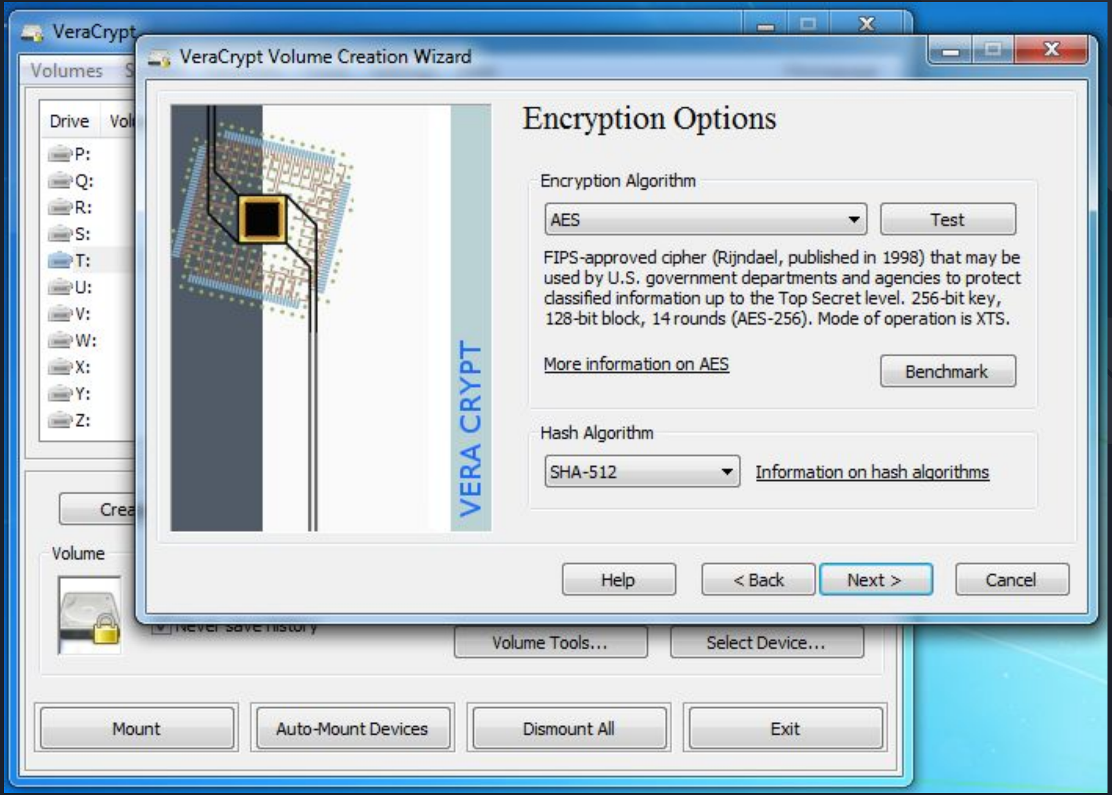
Allow apps downloaded from:

○ App Store

● App Store and identified developers

Click the lock to prevent further changes.

On Windows, Veracrypt



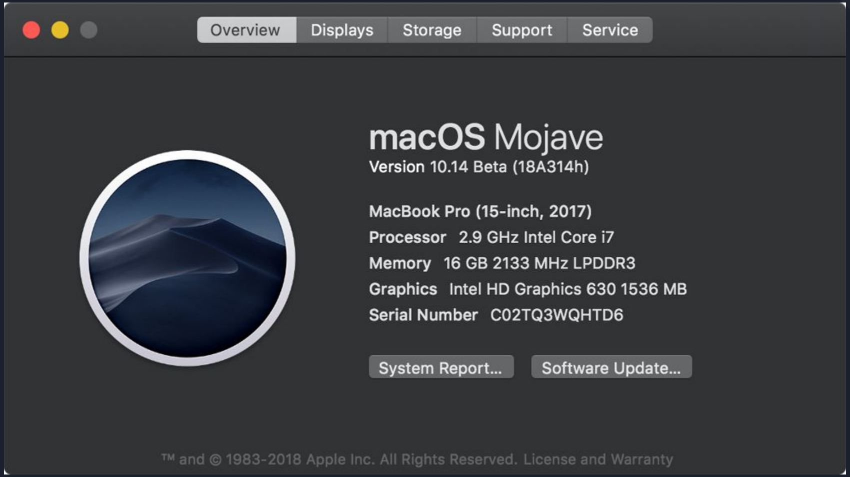
Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: SHA-512

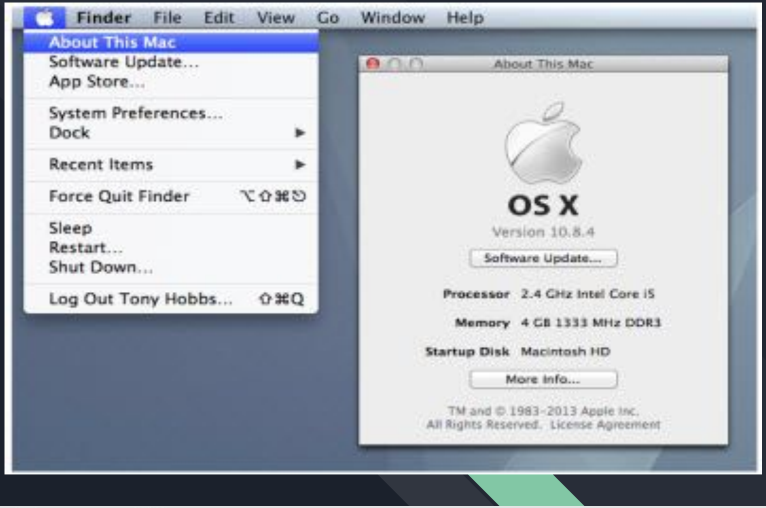
ENABLE ALL SOFTWARE UPDATES



macOS Mojave
Version 10.14 Beta (18A314h)

MacBook Pro (15-inch, 2017)
Processor 2.9 GHz Intel Core i7
Memory 16 GB 2133 MHz LPDDR3
Graphics Intel HD Graphics 630 1536 MB
Serial Number C02TQ3WQHTD6

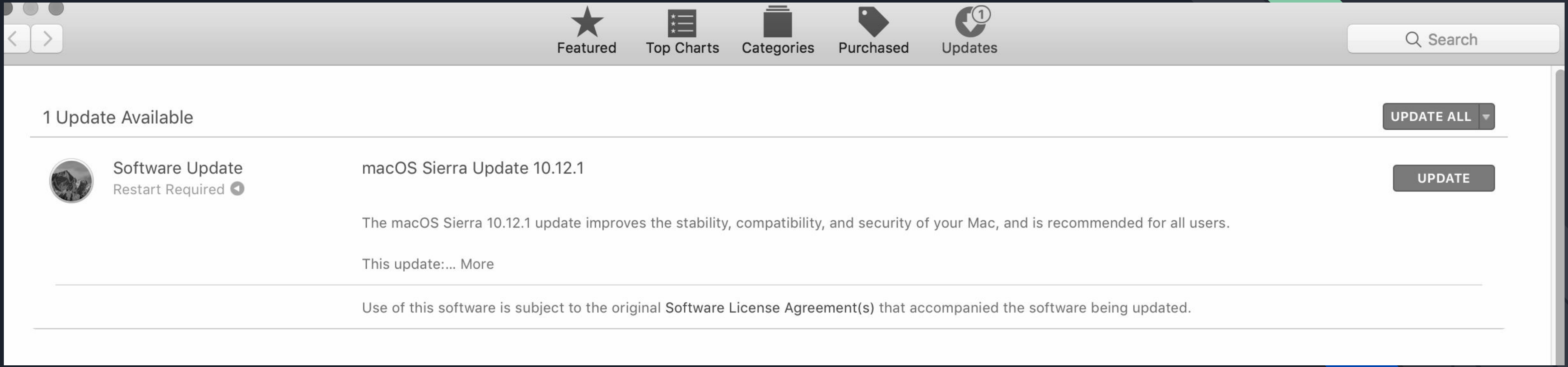
™ and © 1983-2018 Apple Inc. All Rights Reserved. License and Warranty



OS X
Version 10.8.4

Processor 2.4 GHz Intel Core i5
Memory 4 GB 1333 MHz DDR3
Startup Disk Macintosh HD

TM and © 1983-2013 Apple Inc.
All Rights Reserved. License Agreement



1 Update Available

Software Update
Restart Required

macOS Sierra Update 10.12.1

The macOS Sierra 10.12.1 update improves the stability, compatibility, and security of your Mac, and is recommended for all users.

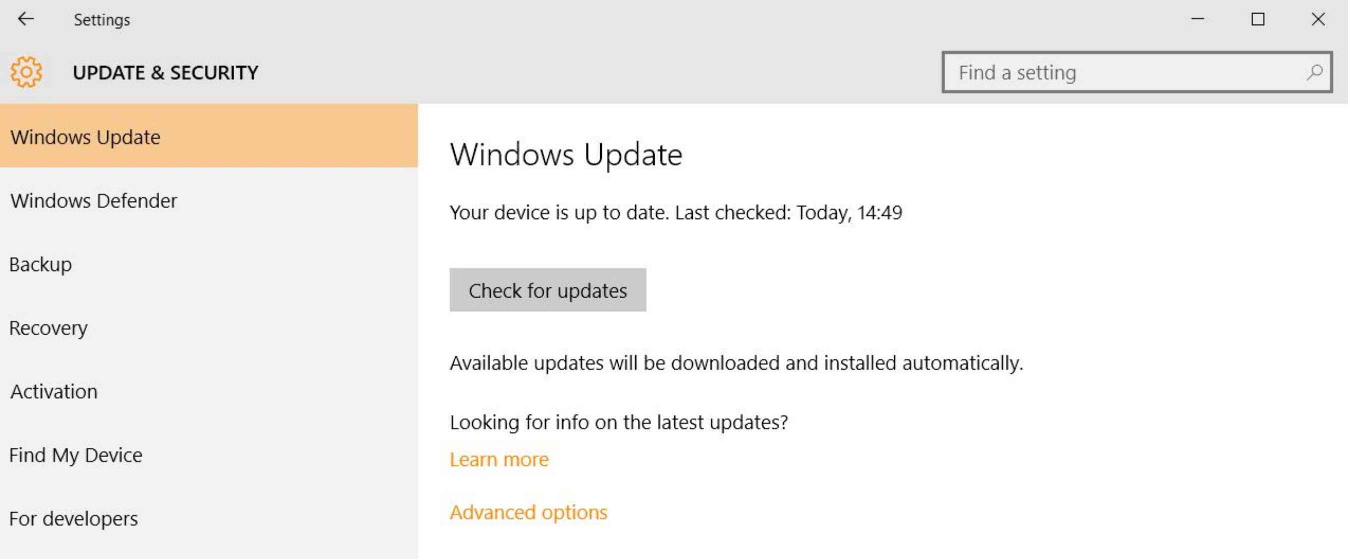
This update:... More

Use of this software is subject to the original Software License Agreement(s) that accompanied the software being updated.

Apple Menu >> App Store

For windows, ensure updates are on:

- Access the search box in your Windows operating system, type **update** and then **Windows Update.**
- Select **Change** settings.
- Click **Install updates automatically (recommended),** in case it is not already selected.



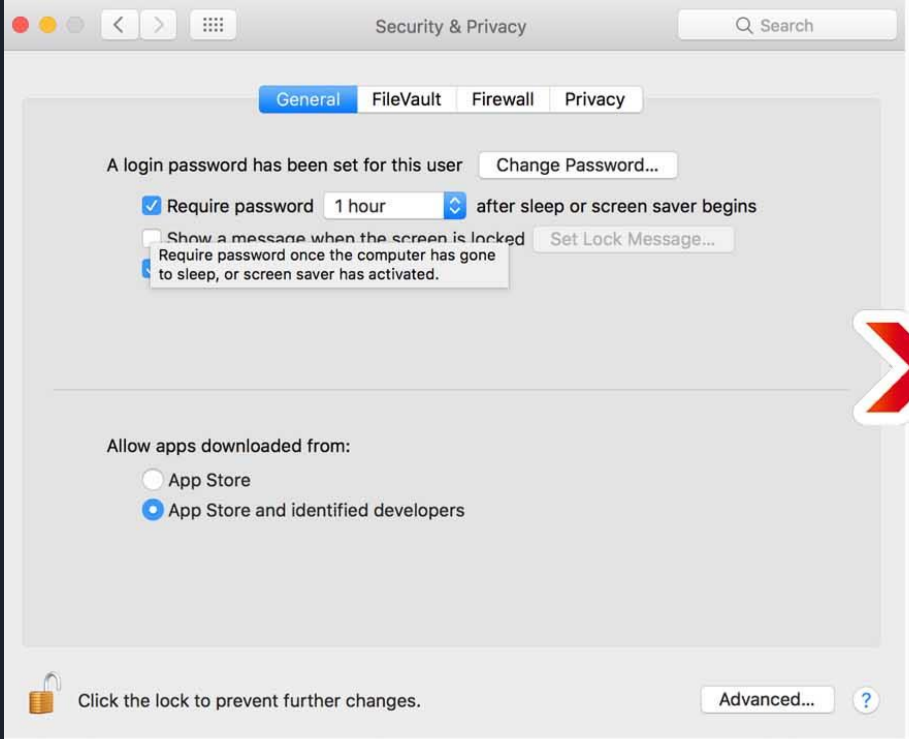
Windows Update

Your device is up to date. Last checked: Today, 14:49

Available updates will be downloaded and installed automatically.

Looking for info on the latest updates?

REVIEW ALL YOUR PRIVACY SETTINGS



A login password has been set for this user Change Password...

☑ Require password 1 hour after sleep or screen saver begins

□ Show a message when the screen is locked Set Lock Message...

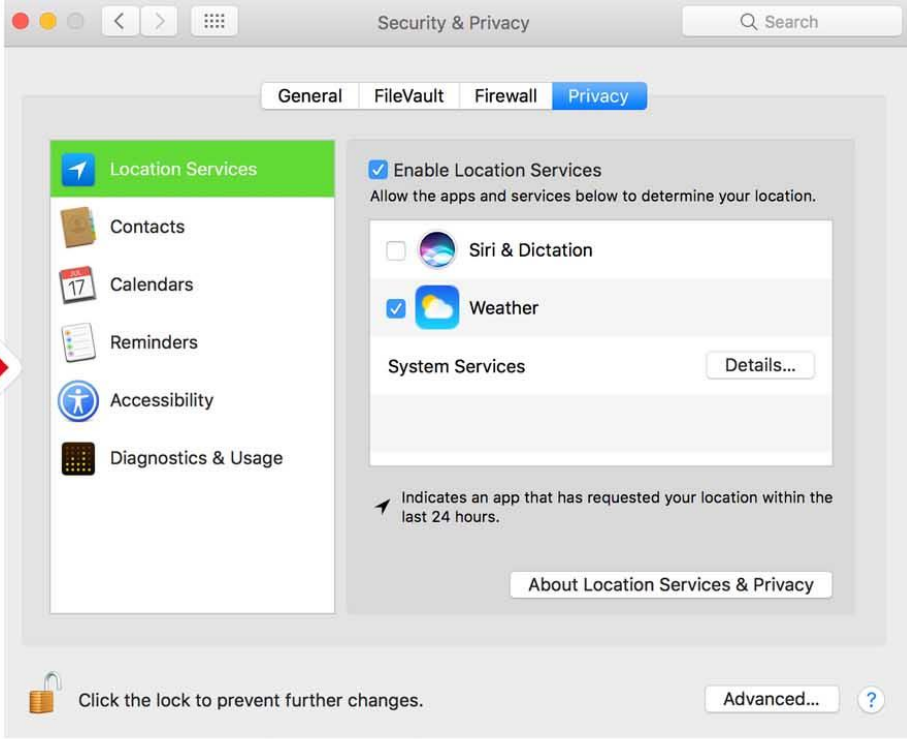
Require password once the computer has gone to sleep, or screen saver has activated.

Allow apps downloaded from:

○ App Store

● App Store and identified developers

Click the lock to prevent further changes. Advanced... ?



☑ Enable Location Services

Allow the apps and services below to determine your location.

□ Siri & Dictation

☑ Weather

System Services Details...

Indicates an app that has requested your location within the last 24 hours.

About Location Services & Privacy

Click the lock to prevent further changes. Advanced... ?

SYSTEM PREFERENCES >> SECURITY PRIVACY

PROTECT YOURSELF FROM MALWARE

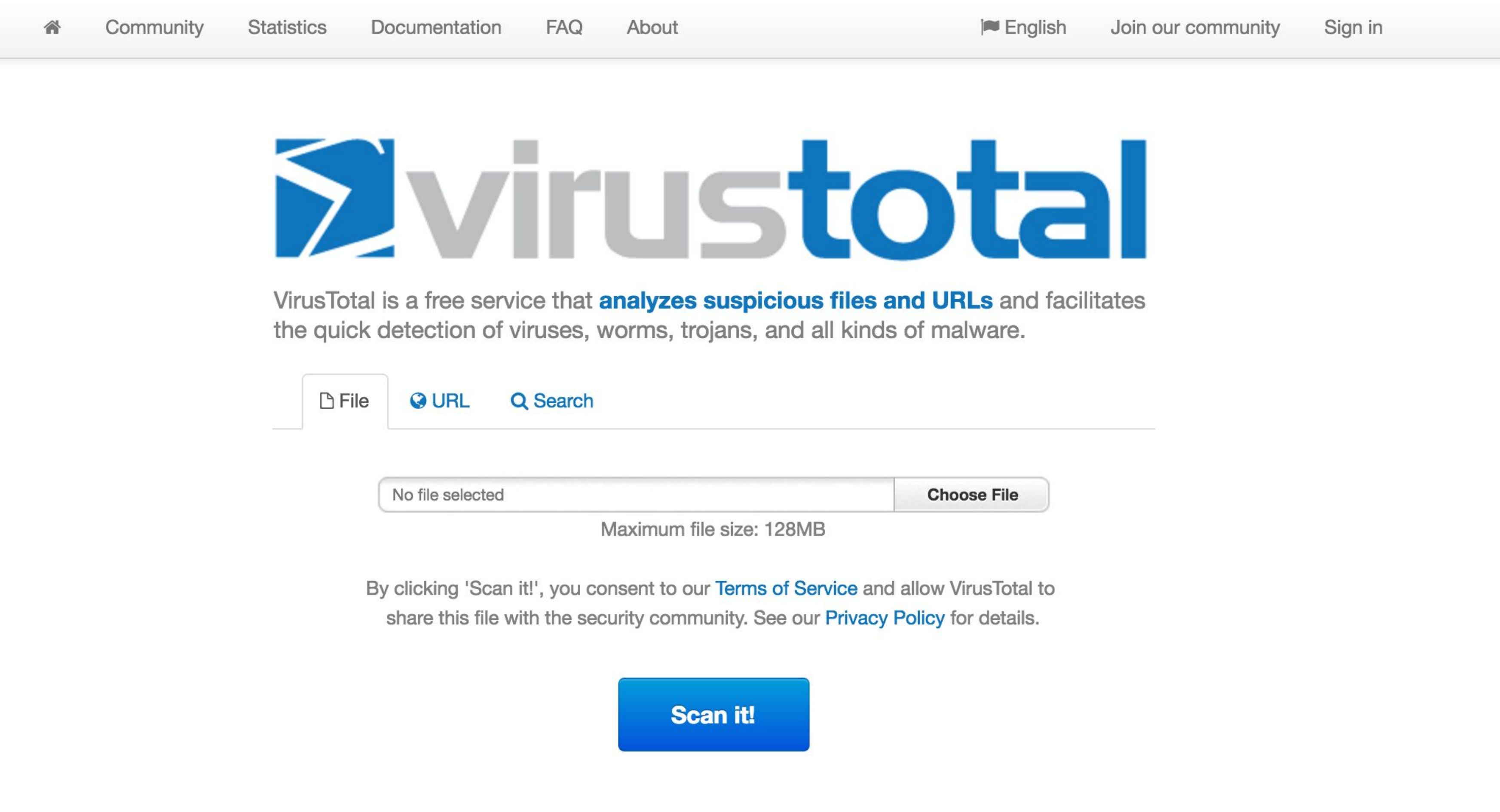
Malware, short for "malicious software," is software that is used to harm computer users. It works in many different ways including, but not limited to, disrupting computer operation, gathering sensitive information, impersonating a user to send spam or fake messages, or gaining access to private computer systems.

The majority of malware is criminal and is most often used to obtain banking information or login credentials for email or social media accounts.

Malware is also used by governments, law enforcement agencies, and even private citizens to circumvent encryption and to spy on users. Malware has wide-range

Malware is one of the number one ways people get their devices compromised. Usually it is through downloading an attachment in email or facebook without scanning it first or opening it in google drive.

SO NEVER OPEN ATTACHMENTS DIRECTLY ALWAYS OPEN IN GOOGLE DRIVE OR DOWNLOAD AND THEN SCAN IN *VIRUSTOTAL.COM*

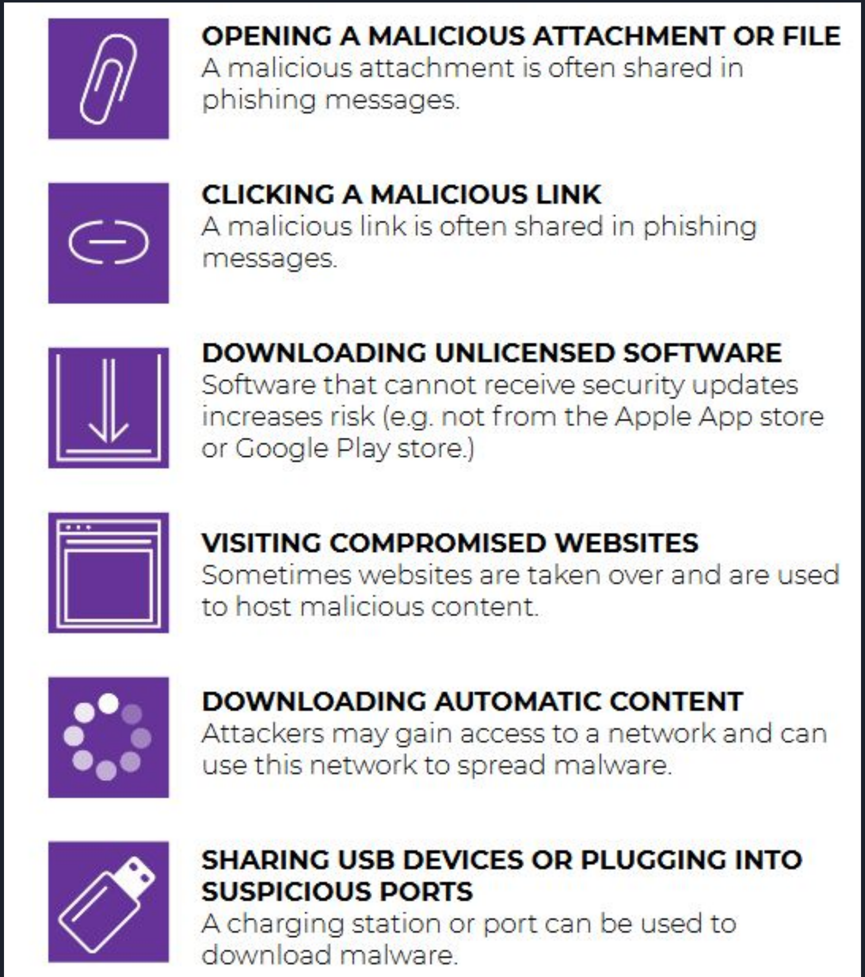


VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Malwarebytes



OPENING A MALICIOUS ATTACHMENT OR FILE
A malicious attachment is often shared in phishing messages.

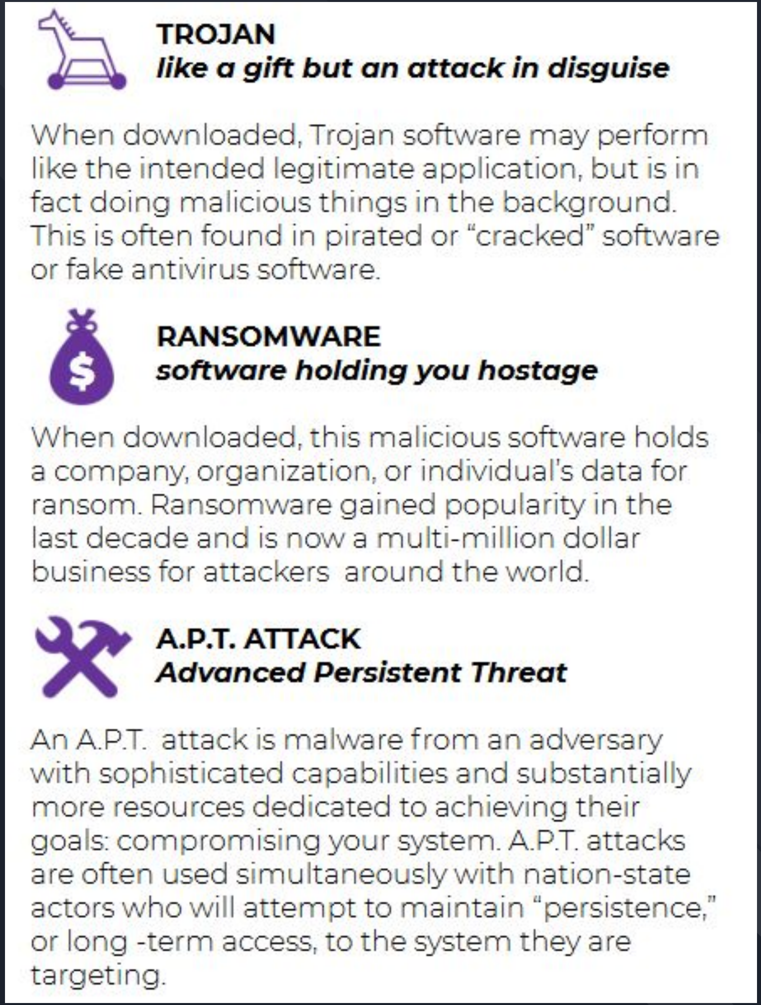
CLICKING A MALICIOUS LINK
A malicious link is often shared in phishing messages.

DOWNLOADING UNLICENSED SOFTWARE
Software that cannot receive security updates increases risk (e.g. not from the Apple App store or Google Play store.)

VISITING COMPROMISED WEBSITES
Sometimes websites are taken over and are used to host malicious content.

DOWNLOADING AUTOMATIC CONTENT
Attackers may gain access to a network and can use this network to spread malware.

SHARING USB DEVICES OR PLUGGING INTO SUSPICIOUS PORTS
A charging station or port can be used to download malware.



TROJAN
like a gift but an attack in disguise

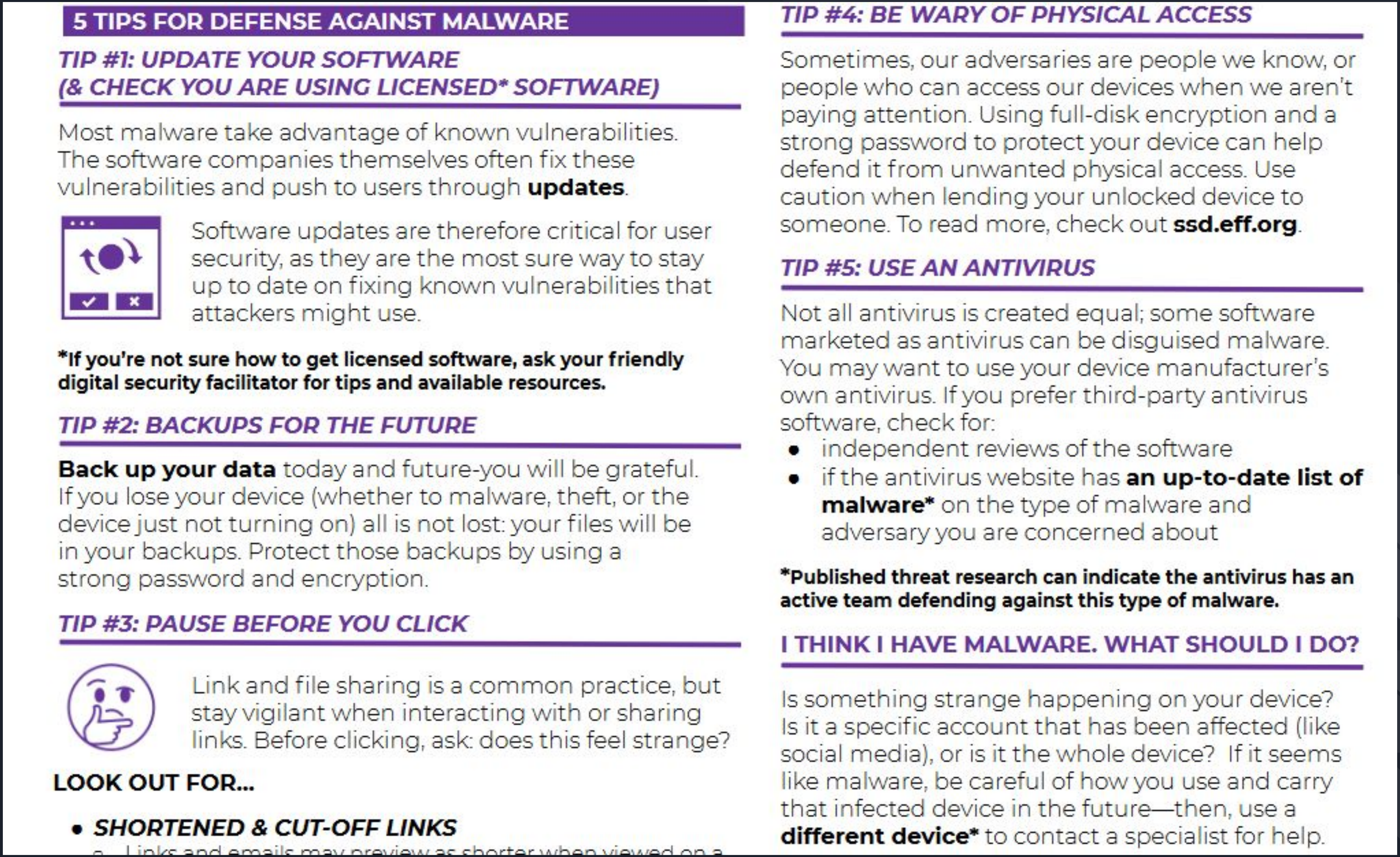
When downloaded, Trojan software may perform like the intended legitimate application, but is in fact doing malicious things in the background. This is often found in pirated or “cracked” software or fake antivirus software.

RANSOMWARE
software holding you hostage

When downloaded, this malicious software holds a company, organization, or individual’s data for ransom. Ransomware gained popularity in the last decade and is now a multi-million dollar business for attackers around the world.

A.P.T. ATTACK
Advanced Persistent Threat

An A.P.T. attack is malware from an adversary with sophisticated capabilities and substantially more resources dedicated to achieving their goals: compromising your system. A.P.T. attacks are often used simultaneously with nation-state actors who will attempt to maintain “persistence,” or long -term access, to the system they are targeting.



5 TIPS FOR DEFENSE AGAINST MALWARE

TIP #1: UPDATE YOUR SOFTWARE (& CHECK YOU ARE USING LICENSED SOFTWARE)*

Most malware take advantage of known vulnerabilities. The software companies themselves often fix these vulnerabilities and push to users through **updates**.

Software updates are therefore critical for user security, as they are the most sure way to stay up to date on fixing known vulnerabilities that attackers might use.

***If you're not sure how to get licensed software, ask your friendly digital security facilitator for tips and available resources.**

TIP #2: BACKUPS FOR THE FUTURE

Back up your data today and future-you will be grateful. If you lose your device (whether to malware, theft, or the device just not turning on) all is not lost: your files will be in your backups. Protect those backups by using a strong password and encryption.

TIP #3: PAUSE BEFORE YOU CLICK

Link and file sharing is a common practice, but stay vigilant when interacting with or sharing links. Before clicking, ask: does this feel strange?

LOOK OUT FOR...

- ***SHORTENED & CUT-OFF LINKS***
  - a. Links and emails may preview as shorter when viewed on a

TIP #4: BE WARY OF PHYSICAL ACCESS

Sometimes, our adversaries are people we know, or people who can access our devices when we aren't paying attention. Using full-disk encryption and a strong password to protect your device can help defend it from unwanted physical access. Use caution when lending your unlocked device to someone. To read more, check out **ssd.eff.org**.

TIP #5: USE AN ANTIVIRUS

Not all antivirus is created equal; some software marketed as antivirus can be disguised malware. You may want to use your device manufacturer's own antivirus. If you prefer third-party antivirus software, check for:

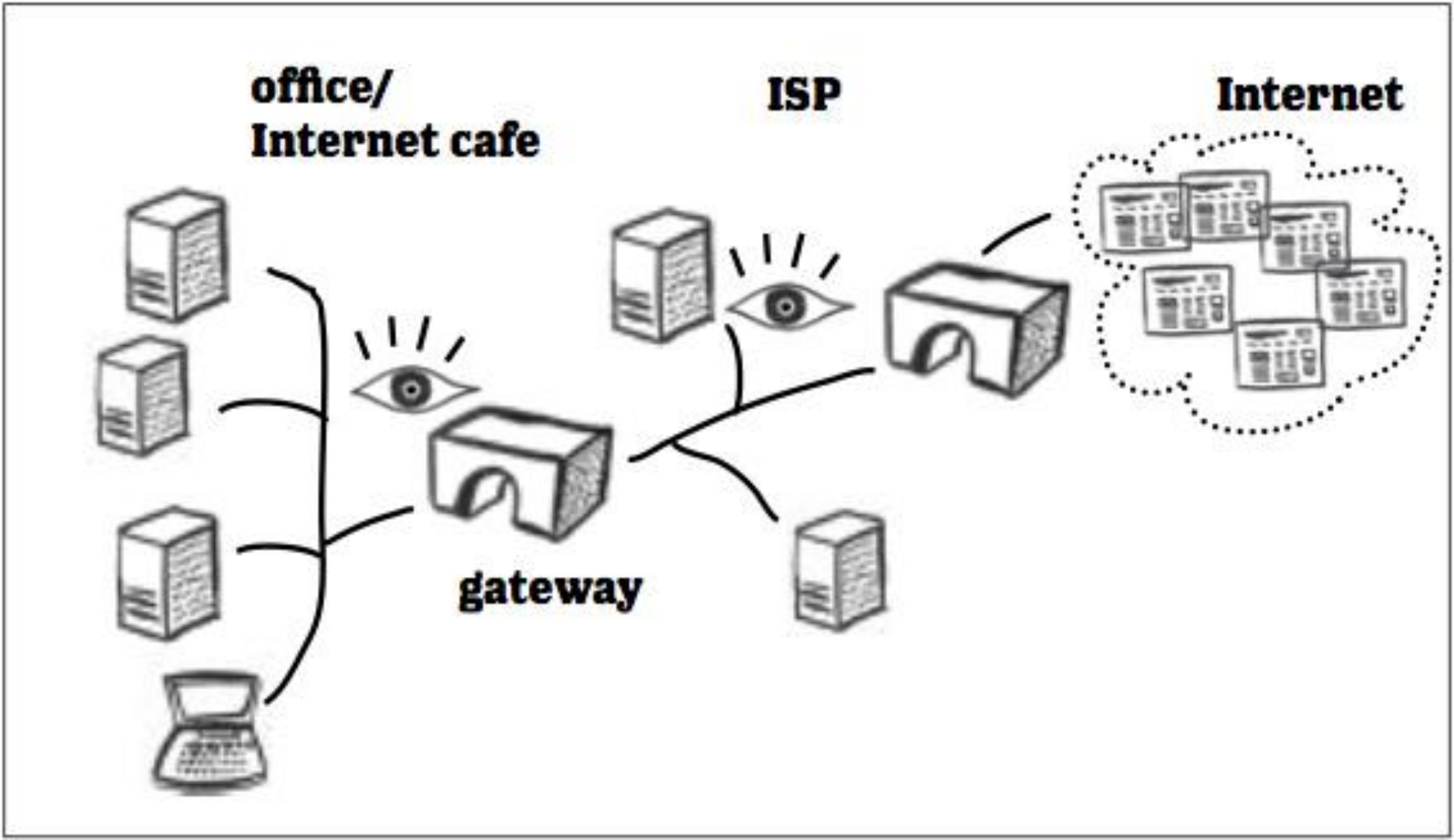
- independent reviews of the software
- if the antivirus website has **an up-to-date list of malware*** on the type of malware and adversary you are concerned about

***Published threat research can indicate the antivirus has an active team defending against this type of malware.**

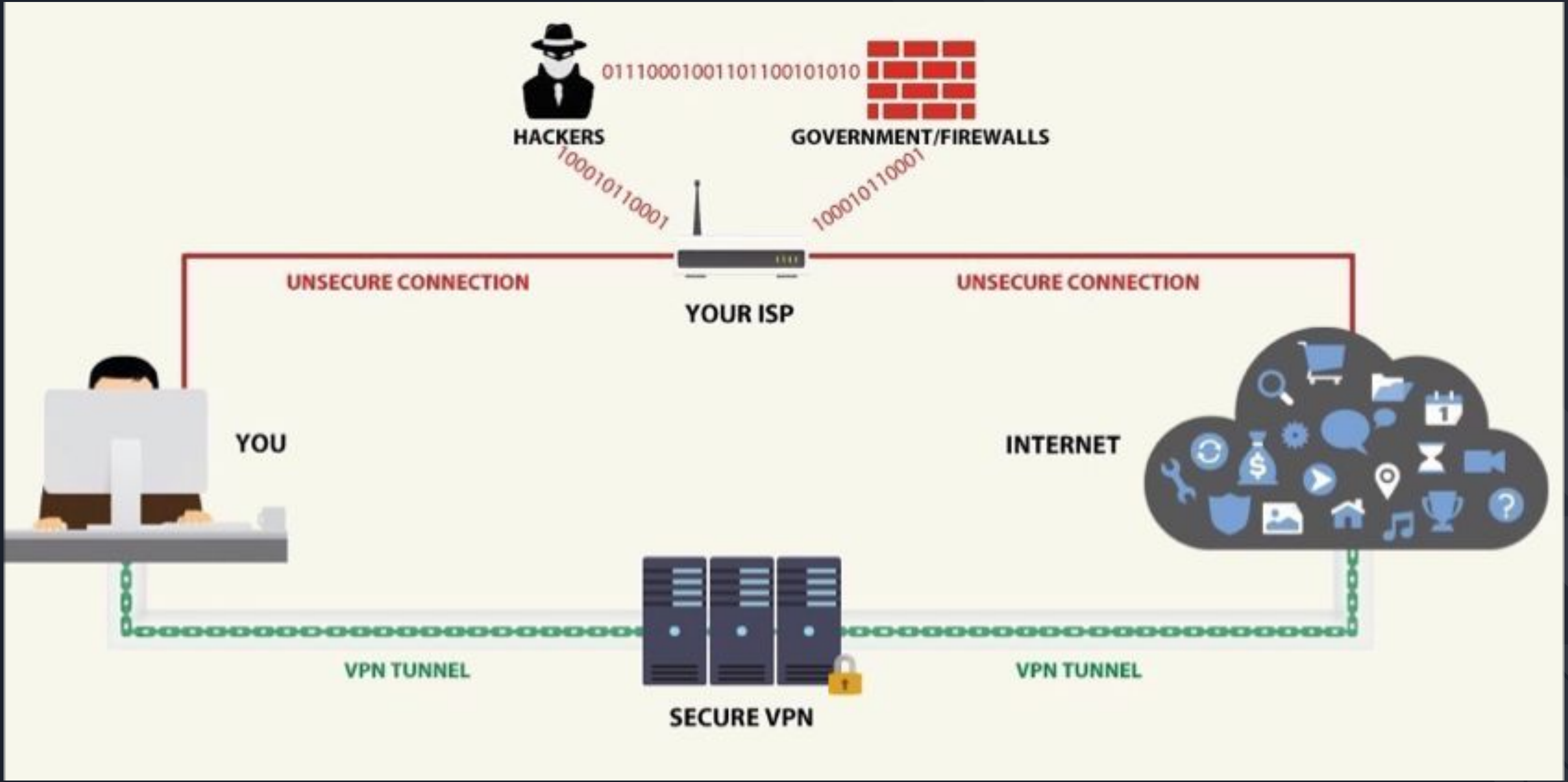
I THINK I HAVE MALWARE. WHAT SHOULD I DO?

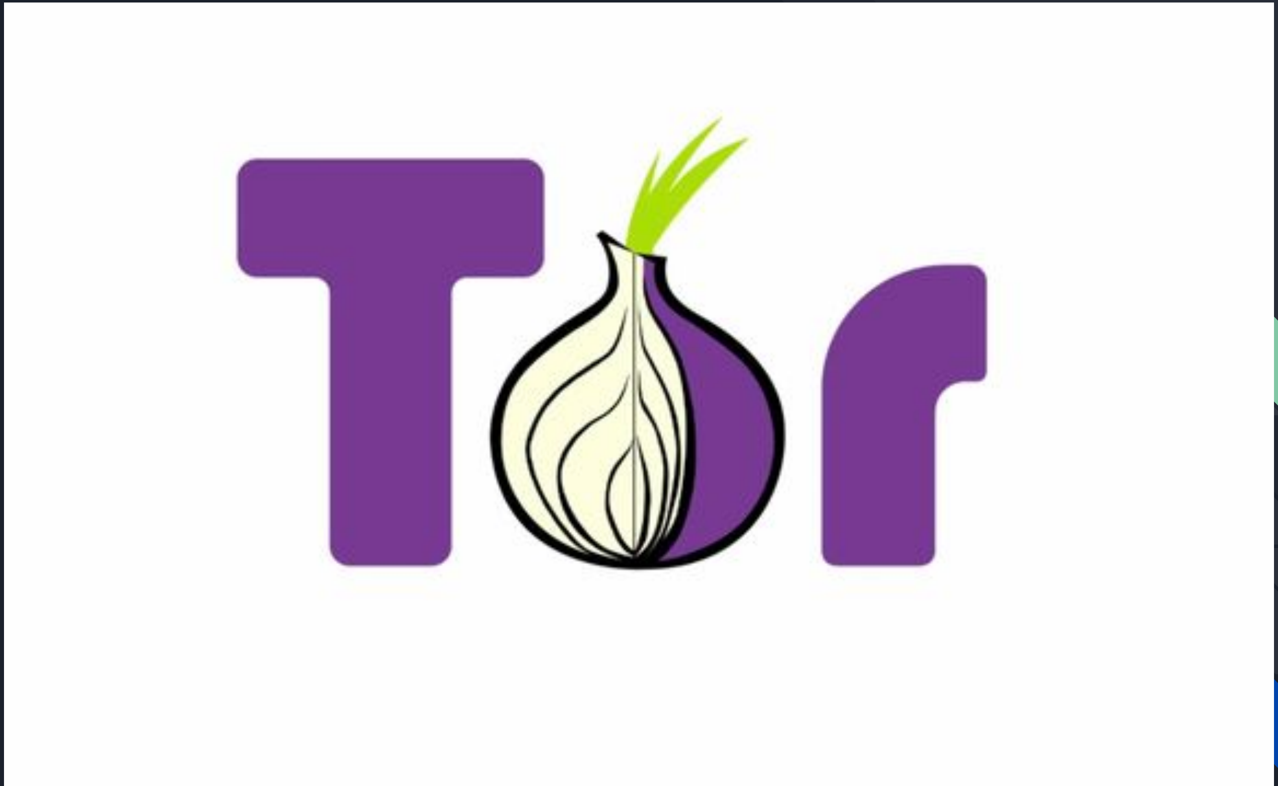
Is something strange happening on your device? Is it a specific account that has been affected (like social media), or is it the whole device? If it seems like malware, be careful of how you use and carry that infected device in the future—then, use a **different device*** to contact a specialist for help.

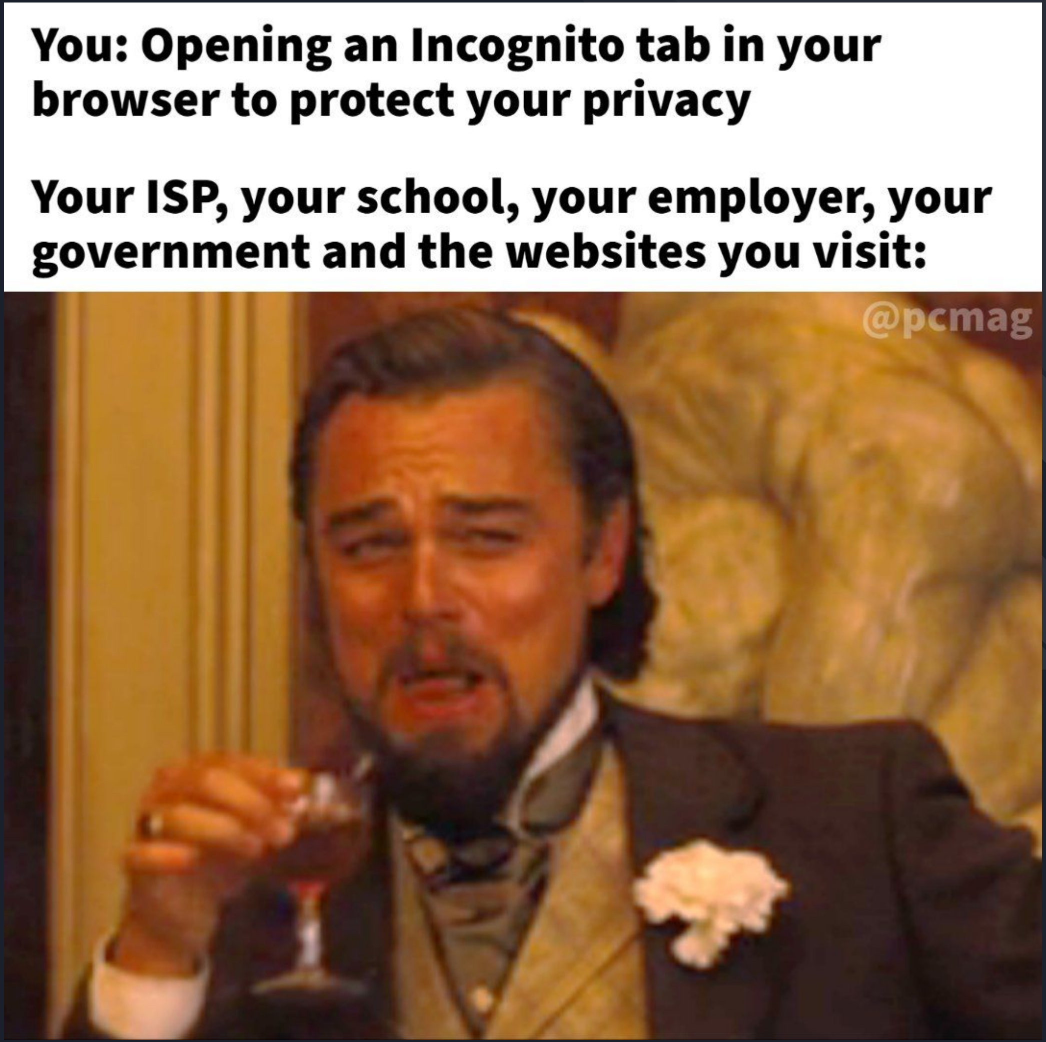
SECURE YOUR NETWORK ACCESS


office/
Internet cafe
ISP
Internet
gateway

* Your Internet traffic is monitored for keywords
* Filtering is implemented directly at the ISP level
*Blocked sites are blacklisted by both their IP addresses and their domain names
* You may be given an unclear or misleading reason to explain why a blocked site fails to load.


HACKERS
01110001001101100101010
GOVERNMENT/FIREWALLS
100010110001
100010110001
UNSECURE CONNECTION
YOUR ISP
UNSECURE CONNECTION
YOU
INTERNET
VPN TUNNEL
SECURE VPN
VPN TUNNEL

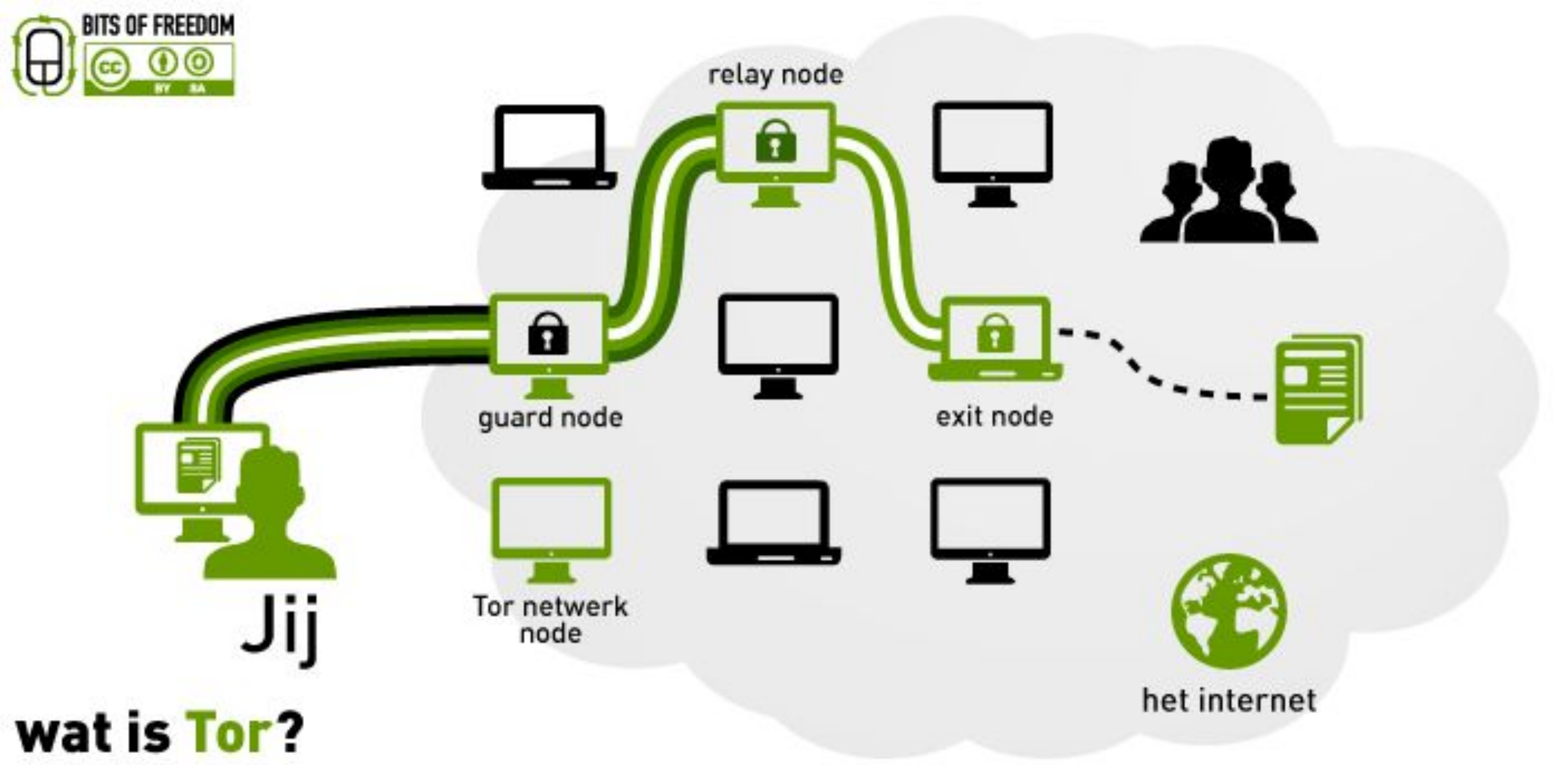

Tor



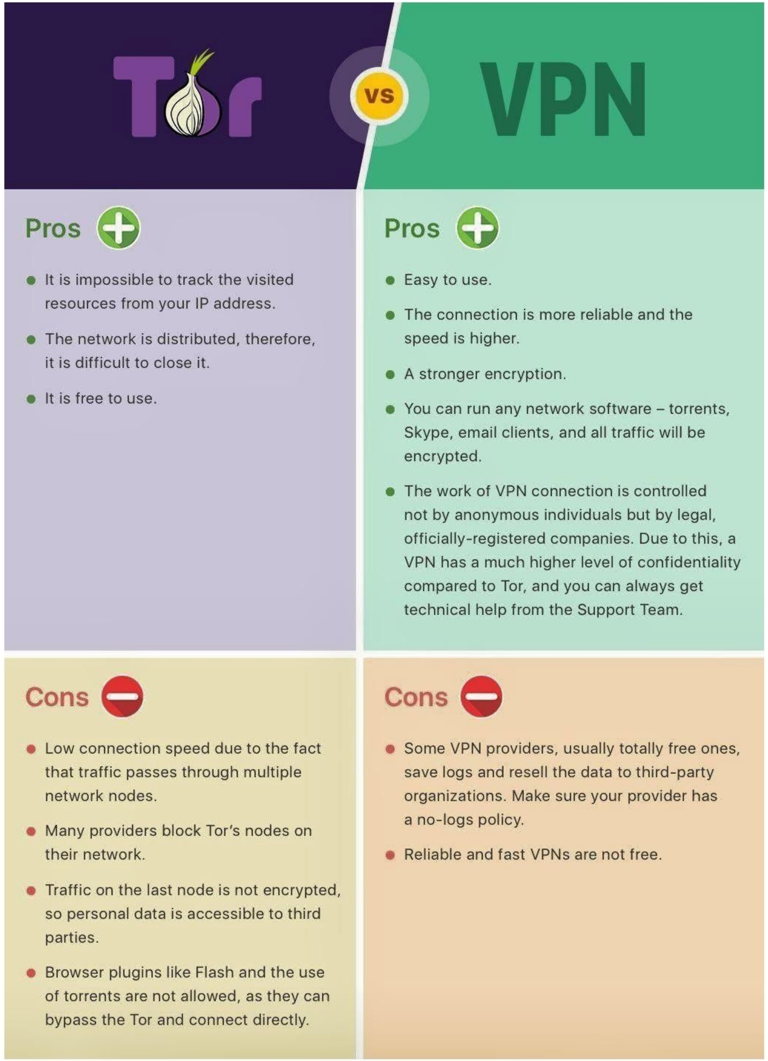
You: Opening an Incognito tab in your browser to protect your privacy

Your ISP, your school, your employer, your government and the websites you visit:

Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms


BITS OF FREEDOM
cc BY SA
relay node
guard node
exit node
Jij
Tor netwerk node
het internet
wat is Tor?

TOR ENTRY AND EXIT NODES ARE PUBLICLY LISTED. YOU NEED TO USE A VPN WITH TOR TO REMAIN ANONYMOUS.



Tor vs VPN

Tor

Pros

- It is impossible to track the visited resources from your IP address.
- The network is distributed, therefore, it is difficult to close it.
- It is free to use.

Cons

- Low connection speed due to the fact that traffic passes through multiple network nodes.
- Many providers block Tor's nodes on their network.
- Traffic on the last node is not encrypted, so personal data is accessible to third parties.
- Browser plugins like Flash and the use of torrents are not allowed, as they can bypass the Tor and connect directly.

VPN

Pros

- Easy to use.
- The connection is more reliable and the speed is higher.
- A stronger encryption.
- You can run any network software – torrents, Skype, email clients, and all traffic will be encrypted.
- The work of VPN connection is controlled not by anonymous individuals but by legal, officially-registered companies. Due to this, a VPN has a much higher level of confidentiality compared to Tor, and you can always get technical help from the Support Team.

Cons

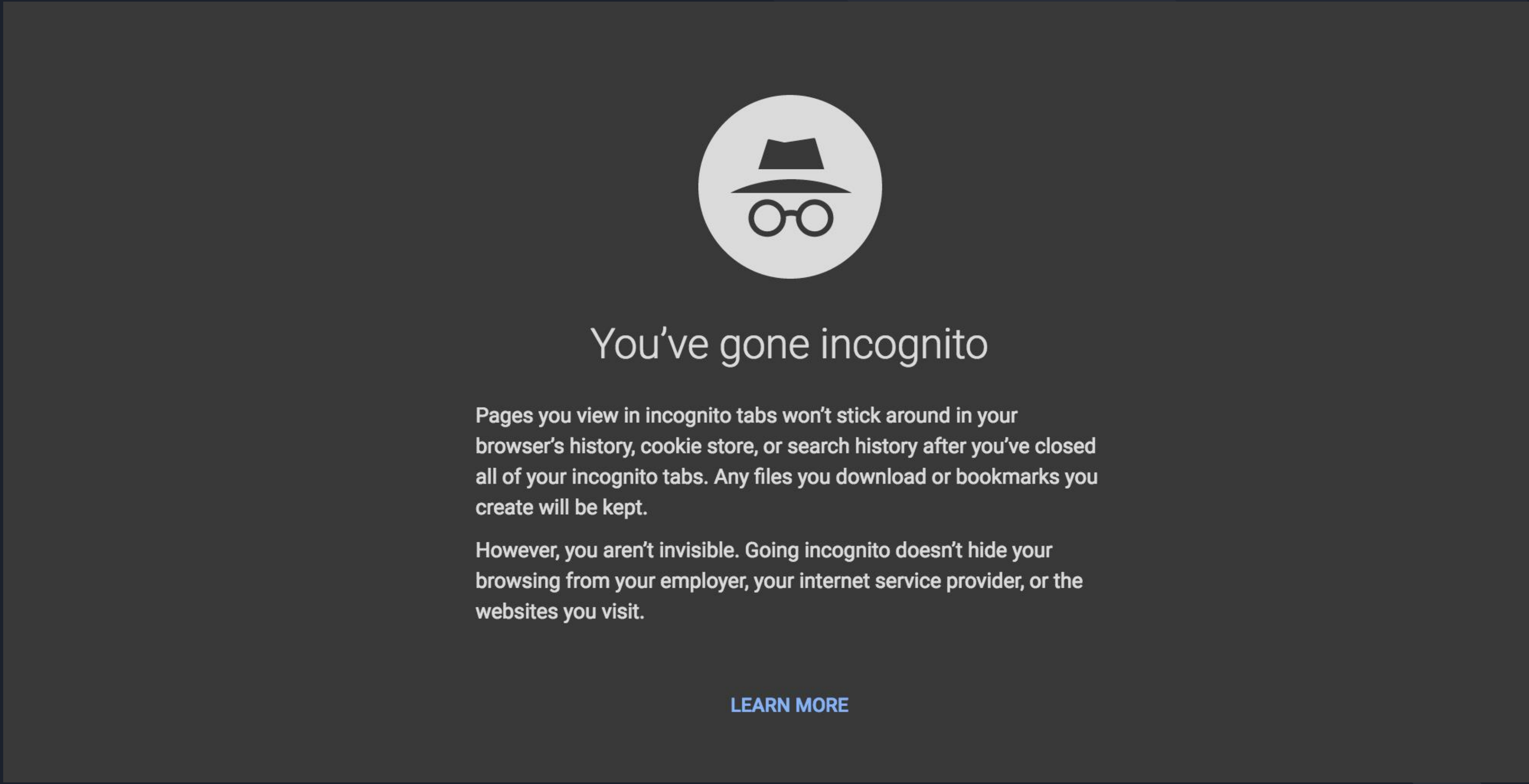
- Some VPN providers, usually totally free ones, save logs and resell the data to third-party organizations. Make sure your provider has a no-logs policy.
- Reliable and fast VPNs are not free.

SECURE YOUR WEB BROWSER

A web browser is a software application used to locate, retrieve and display content on the World Wide Web, including Web pages, images, video and other files.

Browsers we recommend:

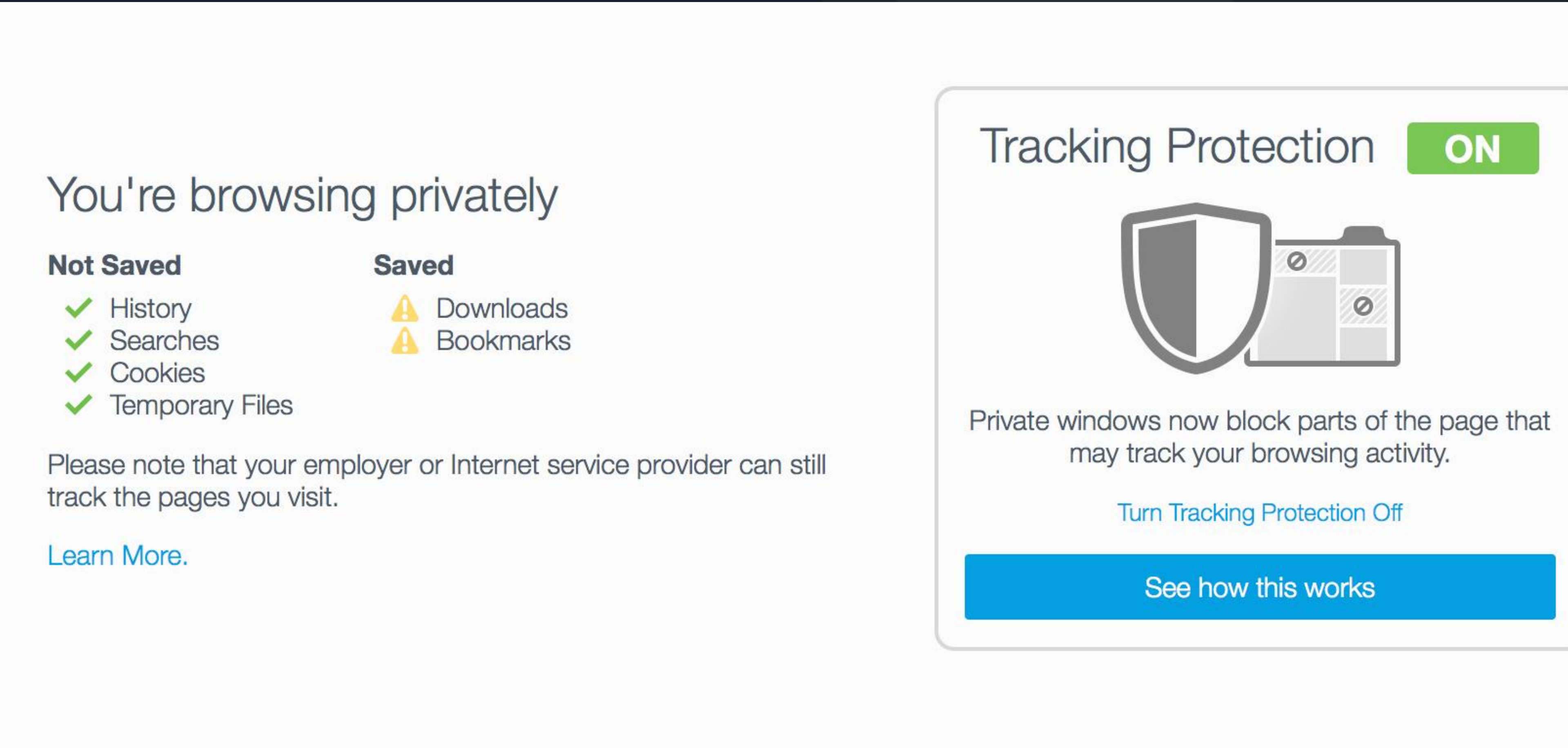
Firefox: https://www.mozilla.org/en-US/firefox/new/
Brave: https://brave.com/
Tor: https://www.torproject.org/
Duck Duck Go: https://duckduckgo.com/



You’ve gone incognito

Pages you view in incognito tabs won’t stick around in your browser’s history, cookie store, or search history after you’ve closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren’t invisible. Going incognito doesn’t hide your browsing from your employer, your internet service provider, or the websites you visit.



You're browsing privately

Not Saved

- ✓ History
- ✓ Searches
- ✓ Cookies
- ✓ Temporary Files

Saved

- ⚠ Downloads
- ⚠ Bookmarks

Please note that your employer or Internet service provider can still track the pages you visit.

Tracking Protection

Private windows now block parts of the page that may track your browsing activity.

HTTPS EVERYWHERE

Available for Mozilla Firefox and Google Chrome, is a popular security tool for online browsing. In a few words, what this extension does is to look for secure versions of the websites you access and use them, instead of their lesser safe versions. If you encounter issues with some websites that don’t work on https://, you simply place that website on a list so that you may access it.

How do advertisers track us across the web?

https://vimeo.com/12204858

PRIVACY BADGER

Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser.

To the advertiser, it's like you suddenly disappeared.

SECURE YOUR SEARCH ENGINE

Duck Duck Go

Cookies: Does not use cookies by default

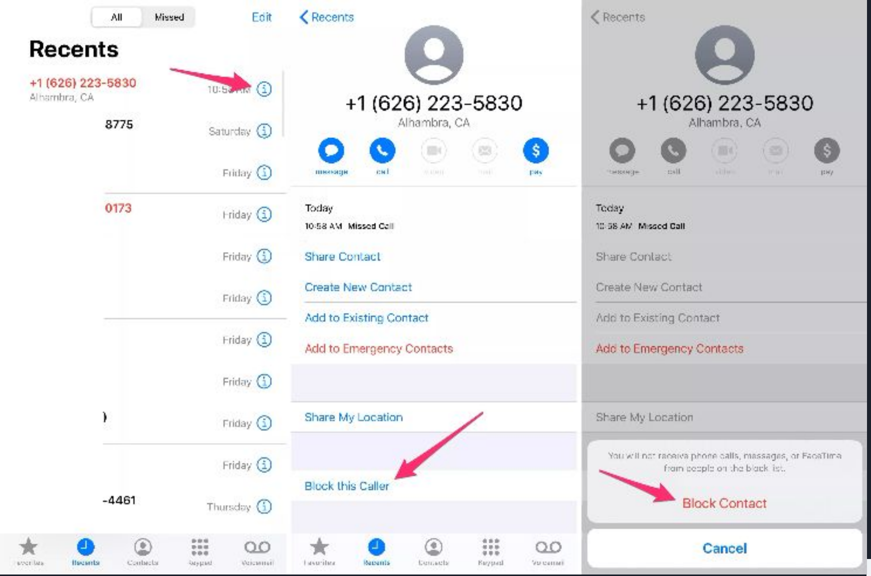
Tracking policy: Does not track and profile users

Personal information: Does not collect or store

Encryption: Yes, HTTPS

COMMUNICATIONS

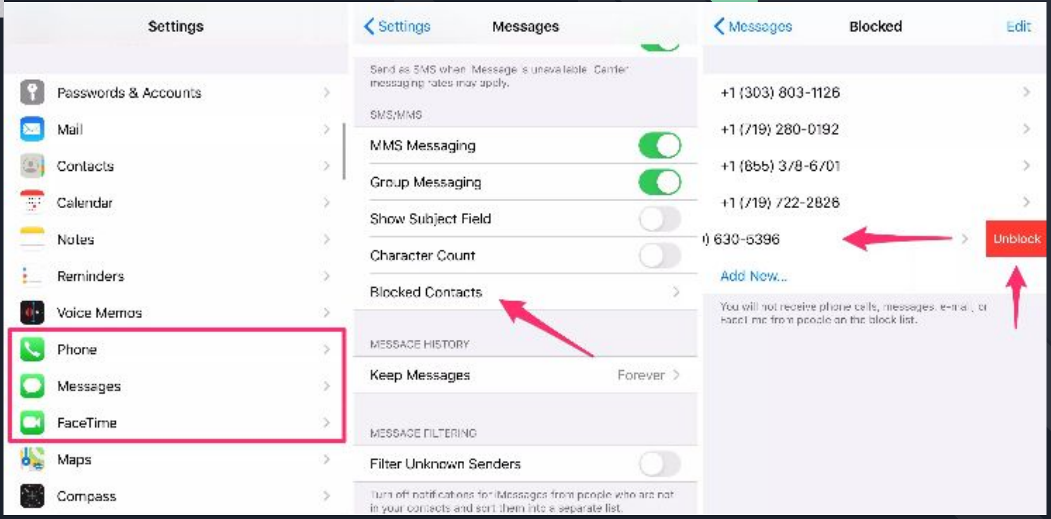
iPhone # Blocking



You will not receive phone calls, messages, or FaceTime from people on the block list.

Block Contact

Cancel



Send as SMS when iMessage is unavailable. Carrier messaging rates may apply.

SMS/MMS

MMS Messaging ●

Group Messaging ●

Show Subject Field ○

Character Count ○

Blocked Contacts

MESSAGE HISTORY

Keep Messages Forever

MESSAGE FILTERING

Filter Unknown Senders ○

Turn off notifications for iMessages from people who are not in your contacts and sort them into a separate list.

+1 (303) 803-1126

+1 (719) 280-0192

+1 (855) 378-6701

+1 (719) 722-2826

) 630-5396 Unblock

Add Now...

You will not receive phone calls, messages, e-mail, or FaceTime from people on the block list.

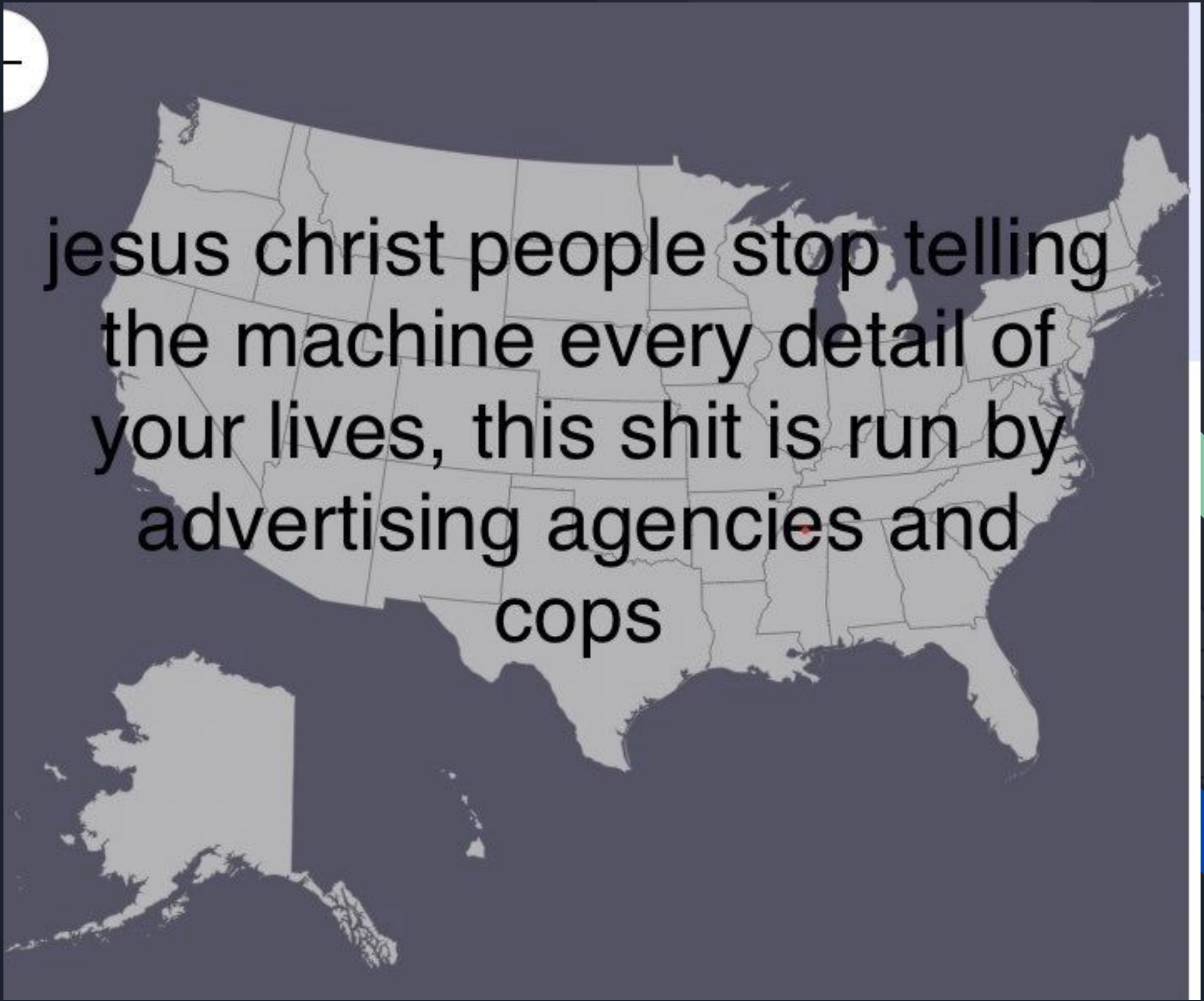
SIGNAL

Signal’s privacy policy is short and concise. Unlike WhatsApp, Signal doesn’t store any message metadata. The closest piece of information to metadata that the Signal server stores is the last time each user connected to the server, and the precision of this information is reduced to the day, rather than the hour, minute, and second.

WIRE

Wire offers the most comprehensive collaboration suite featuring messenger, voice, video, conference calls, file-sharing, and external collaboration – all protected by the most secure end-to-end-encryption.

ONLINE IDENTITY



jesus christ people stop telling the machine every detail of your lives, this shit is run by advertising agencies and cops

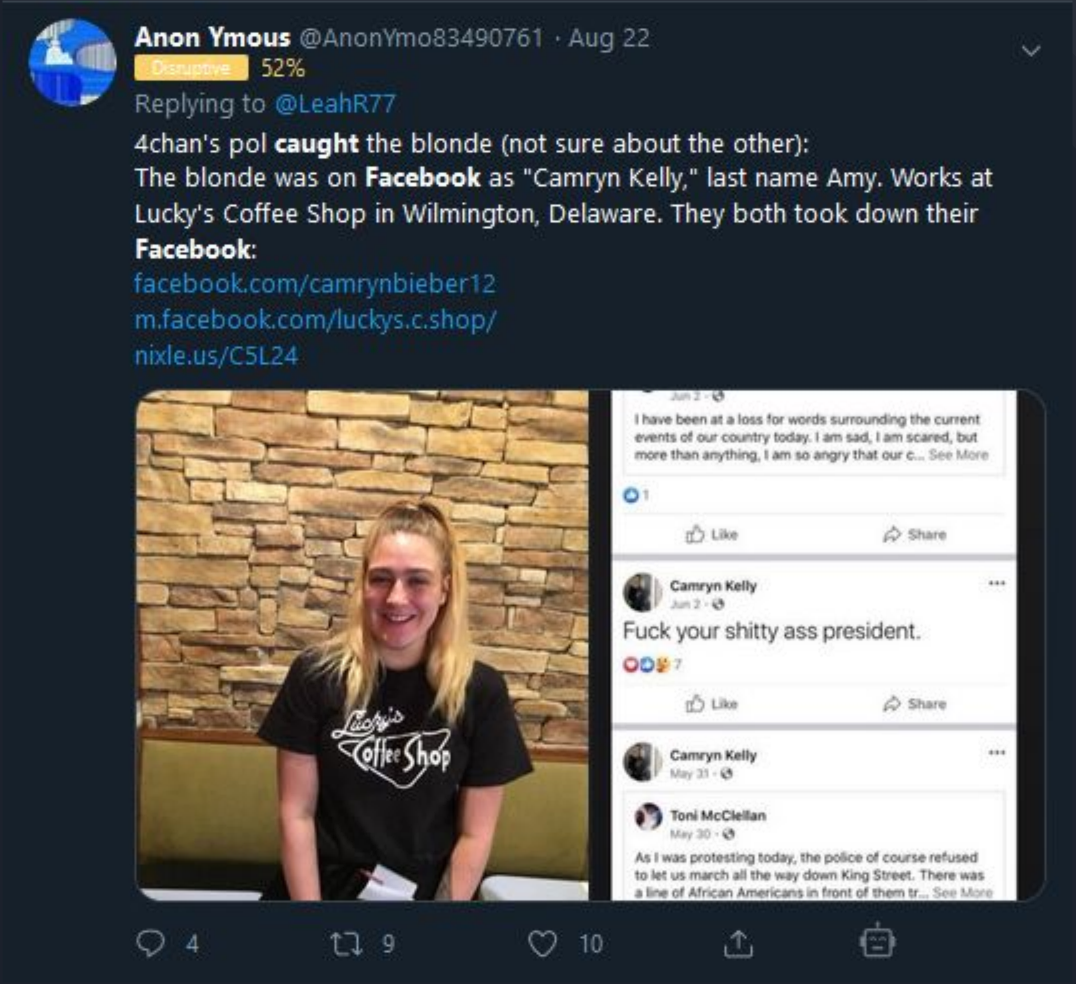
Option 1: Poison Your Data
Option 2: Delete Your Data
Option 3: Make Your Data Private
Option 4: Nuke it all

Understand start to finish, who can see what when we create a sockpuppet.

FACEBOOK

Facebook Profile Settings

- Go to your profile and then click on “About” underneath your top cover photo
- Go to your profile and click on “More” underneath your top cover photo
- Under the very top navigation, at the far right is a small triangle, click on it to reveal a drop down. Then click on “Settings”



Anon Ymous @AnonYmo83490761 · Aug 22

Disruptive 52%

Replying to @LeahR77

4chan's pol **caught** the blonde (not sure about the other):
The blonde was on **Facebook** as "Camryn Kelly," last name Amy. Works at Lucky's Coffee Shop in Wilmington, Delaware. They both took down their **Facebook**:
facebook.com/camrynbieber12
m.facebook.com/luckys.c.shop/
nixle.us/C5L24

Jun 2 ·

I have been at a loss for words surrounding the current events of our country today. I am sad, I am scared, but more than anything, I am so angry that our c... See More

1

Like Share

Camryn Kelly
Jun 2 ·

Fuck your shitty ass president.

7

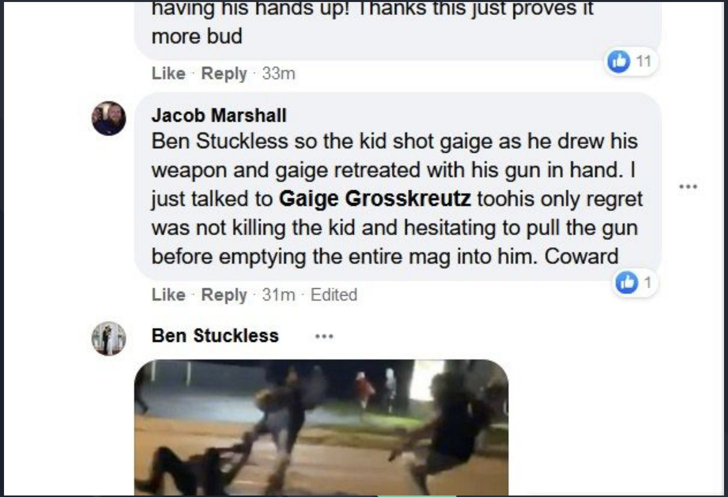
Like Share

Camryn Kelly
May 31 ·

Toni McClellan
May 30 ·

As I was protesting today, the police of course refused to let us march all the way down King Street. There was a line of African Americans in front of them tr... See More

4 9 10



having his hands up! Thanks this just proves it more bud

Like · Reply · 33m 11

Jacob Marshall
Ben Stuckless so the kid shot gaige as he drew his weapon and gaige retreated with his gun in hand. I just talked to **Gaige Grosskreutz** toohis only regret was not killing the kid and hesitating to pull the gun before emptying the entire mag into him. Coward

Like · Reply · 31m · Edited 1

Ben Stuckless ···

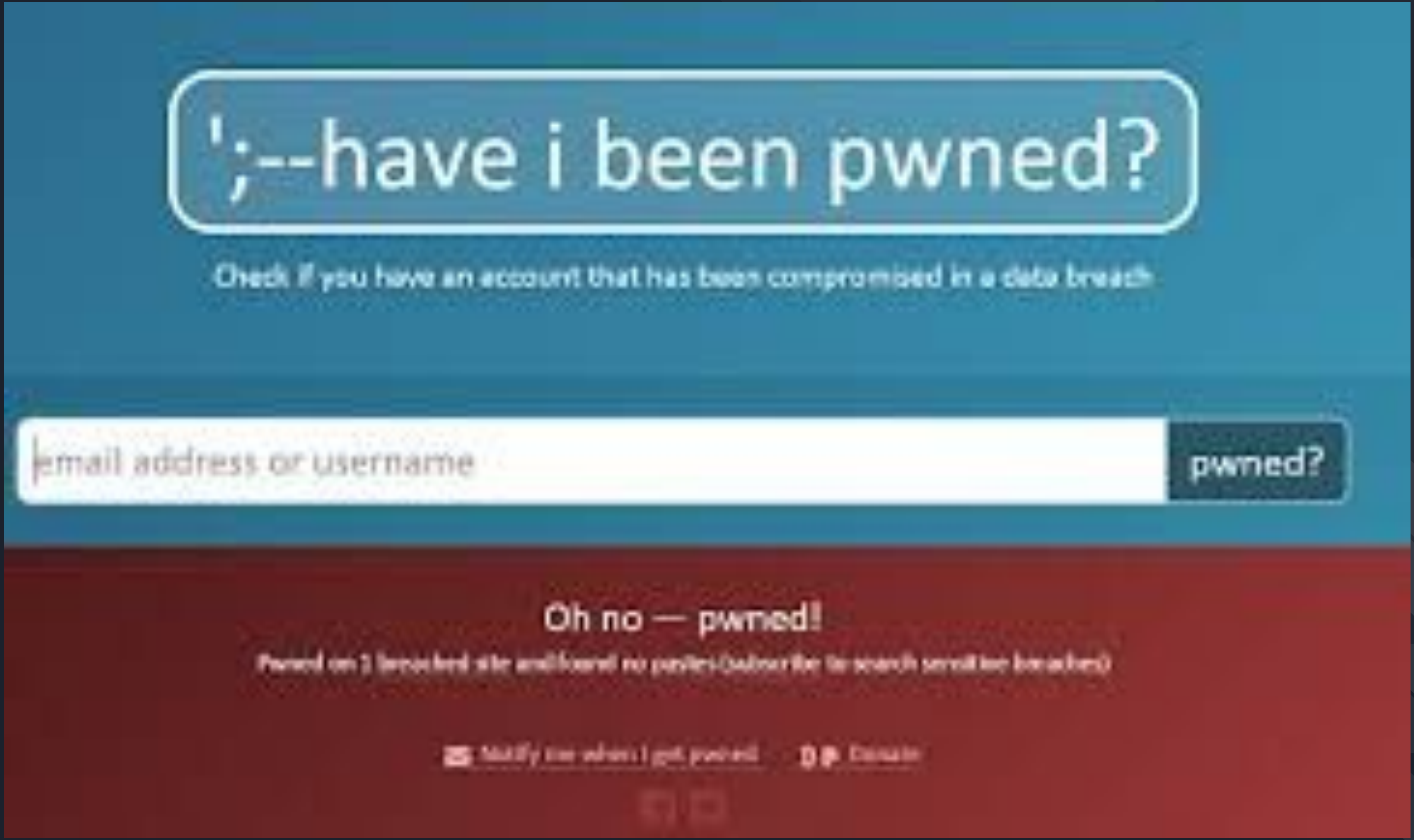
Google Profile Settings

- Go to https://myactivity.google.com/myactivity
- Go to https://aboutme.google.com
- Go to https://myaccount.google.com/privacy

LinkedIn Profile Settings

- Click on your profile, on the right side click on “Edit your public profile”
  - Click on “make my public profile visible to no one”, this will disable search engines from indexing your profile (https://www.linkedin.com/public-profile/settings)
  - “Edit public profile URL”: make sure the url does not contain your real name
- On the top navigation settings, click Me -> Settings & Privacy
  - Scroll to Partners and Third Parties - Turn off anything in this section (https://www.linkedin.com/psettings/third-party-applications)

Doxxing is releasing people's personal information and using it to hurt them.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

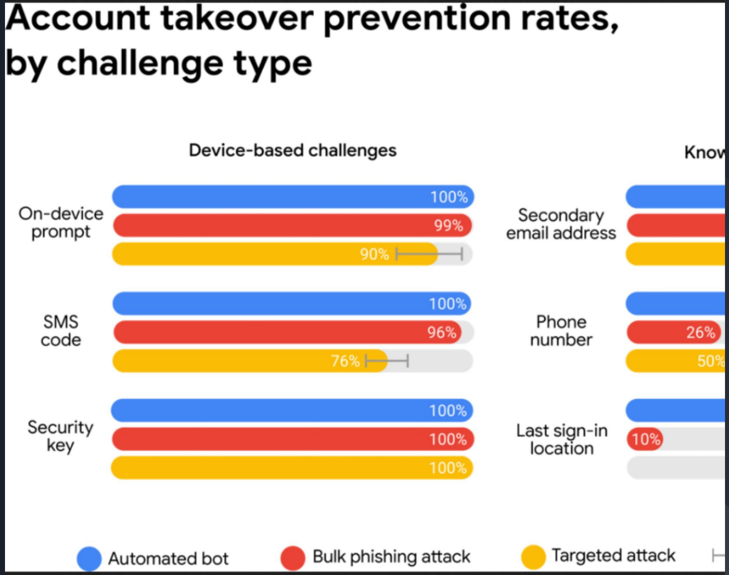
TURN ON 2-FACTOR AUTHENTICATION

2 Factor Authorization (2FA) is used in addition to a password. Often times, you will be able to enable SMS messages to your mobile phone if a strange log-in to your account happens. This goes a long, long way in preventing hacked accounts.

We recommend you enable this for your gmail, facebook, twitter, and banking accounts.

You can find 2FA for lots of sites at https://www.turnon2fa.com/tutorials/

U2F/FIDO2 > TOTP > no 2FA > SMS 2FA Real 2FA is better than none, and SMS is worse than none.



Account takeover prevention rates, by challenge type

* Make a list (write it down) of all of your social media profiles.

* This isn’t just twitter and facebook. Your instagram. Etsy. LinkedIn. Couchsurfers. Fetlife.

* Your old backpages ad. Etc. Of these, facebook and linkedin are probably the most common offenders but you need to check all of them and just delete the ones you don’t need any more.

* Even if the information is outdated, it could still be used to confirm or sift through other evidence found elsewhere.

Opt-out of people finders (counter-doxxing)

- Axciom: https://isapps.acxiom.com/optout/optout.aspx
- BeenVerified: https://www.beenverified.com/faq/opt-out/
- InfoTracer: https://infotracer.com/optout/
- CheckPeople: http://www.checkpeople.com/optout
- Instant Checkmate: https://www.instantcheckmate.com/optout/
- Intelius: https://www.intelius.com/optout.php
- LexisNexis: https://www.lexisnexis.com/privacy/directmarketingopt-out.aspx
- PeekYou: http://www.peekyou.com/about/contact/optout/index.php
- PeopleFinders: http://www.peoplefinders.com/manage/
- PeopleSmart: https://www.peoplesmart.com/optout-signup
- Pipl: https://pipl.com/directory/remove/
- PrivateEye: http://secure.privateeye.com/help/default.aspx#26
- PublicRecords360: http://www.publicrecords360.com/optout.html
- Radaris: http://radaris.com/page/how-to-remove
- Spokeo: http://www.spokeo.com/opt_out/new
- USA People Search: http://www.usa-people-search.com/manage/default.aspx
- US Search: http://www.ussearch.com/privacylock
- TruthFinder.com: https://www.truthfinder.com/opt-out/
- Whitepages: https://www.whitepages.com/suppression_requests
- Nuwber: https://nuwber.com/removal/link
- OneRep: https://onerep.com/optout
- MyLife: https://www.mylife.com/privacy-policy
- FamilyTreeNow: http://www.familytreenow.com/
- A more comprehensive list available at Trollbusters: https://yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites/

https://www.wired.com/story/opt-out-data-broker-sites-privacy/

https://www.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo

Personal
Data

What does google know about you?

https://myactivity.google.com

http://www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete/

COMPARTMENTALISATION

PROFESSIONAL ACCOUNT

- Links and resources
- Positions on academic focus
- No explicit political positions
- And comments should be private or set for students

PERSONAL ACCOUNT

- Marital status
- Sexual orientation
- Personal opinions
- No students allowed

PROTECT YOURSELF FROM IDENTITY ATTACKS (PHISHING)

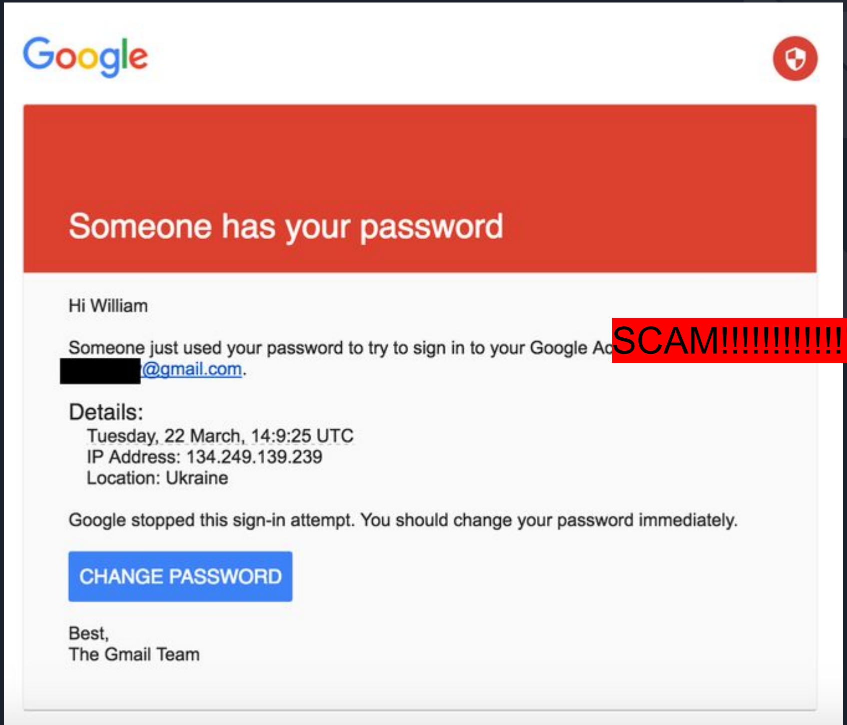
✓PHISHING

Phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. All phishing attacks are fundamentally a social engineering attack, where they differ is in their implementation and targeting. Phishing attacks are becoming more and more sophisticated, it's important to stay aware of all the new (and old) forms of attack. When it comes down to it, if something smells fishy, use caution.

- Cat phishing: a person using a fake identity to try and extract information from a target. Often implemented on dating sites, but also over social networks.
- Spear phishing: a more specific form of phishing, the attacker uses available information about you to direct their attack directly at you. A custom attack targeting you for specific information, usually financial details.
- Vishing: Voice based and mass distributed scamming over phone or voice message social network messages.
- Smishing: SMS based and mass distributed scamming over text messages or social network messages.
- Pharming: An imposter website may be set up to collect your data by masquerading as a legitimate website, an example could be something like: microsotf.com VS microsoft.com

- The message contains a mismatched URL, or a misleading domain name
- The message is coming from your friend, but doesn’t sound like your friend
- The message asks for personal information like banking information, or wants you to change your password
- You didn't initiate the action
- You're asked to send money to cover expenses
- The message appears to be from a government agency

NEVER EVER *EVER* RESPOND TO A REQUEST FOR YOUR PASSWORD SENT BY EMAIL, even if the request appears legitimate. -- sincerely, the Democratic National Committee



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Ac [redacted]@gmail.com.

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

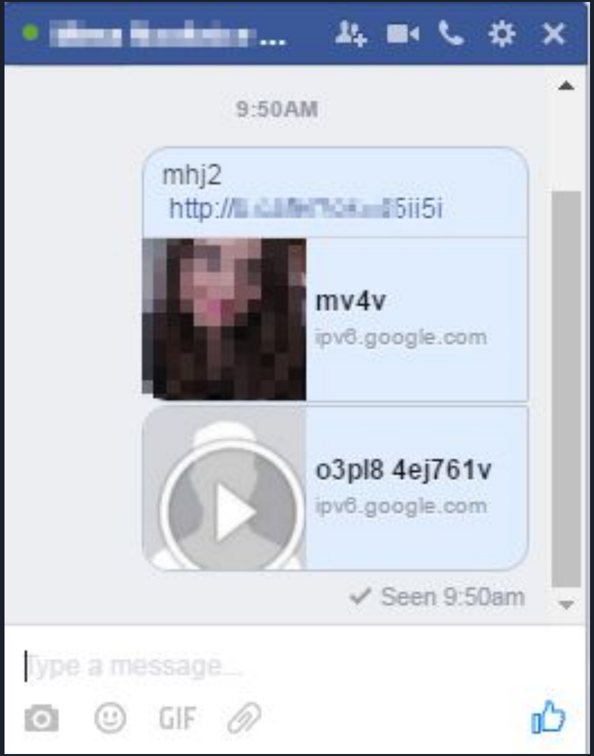
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

SCAM!!!!!!!!!!!!!!

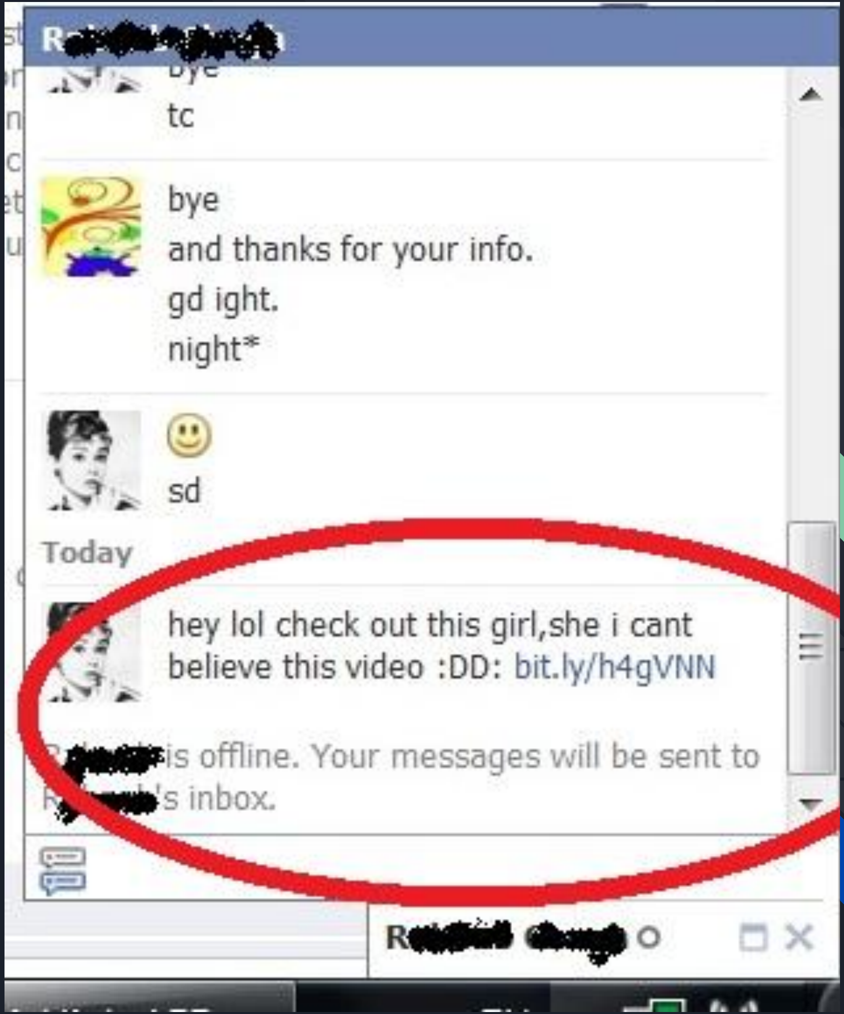
"This is a legitimate email," Charles Delavan, a Clinton campaign aide, replied to another of Mr. Podesta's aides, who had noticed the alert. "John needs to change his password immediately."



mhj2
http://[redacted]5ii5i

mv4v
ipv6.google.com

o3pl8 4ej761v
ipv6.google.com



bye
tc

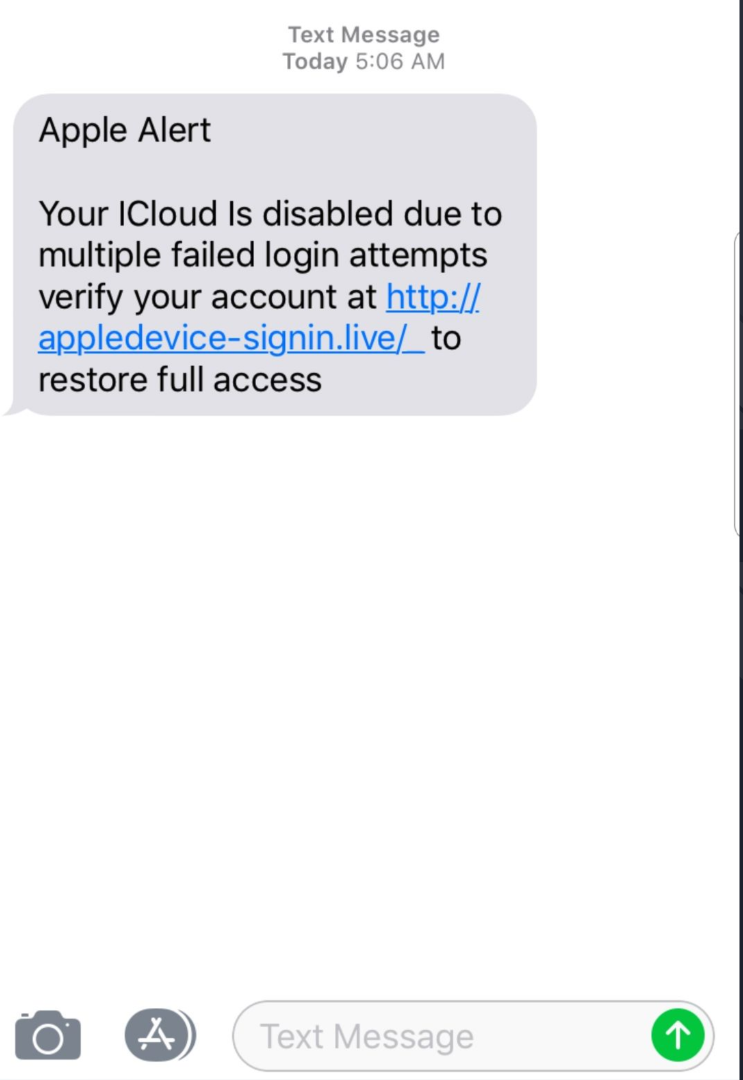
bye
and thanks for your info.
gd ight.
night*

🙂
sd

Today

hey lol check out this girl,she i cant believe this video :DD: bit.ly/h4gVNN

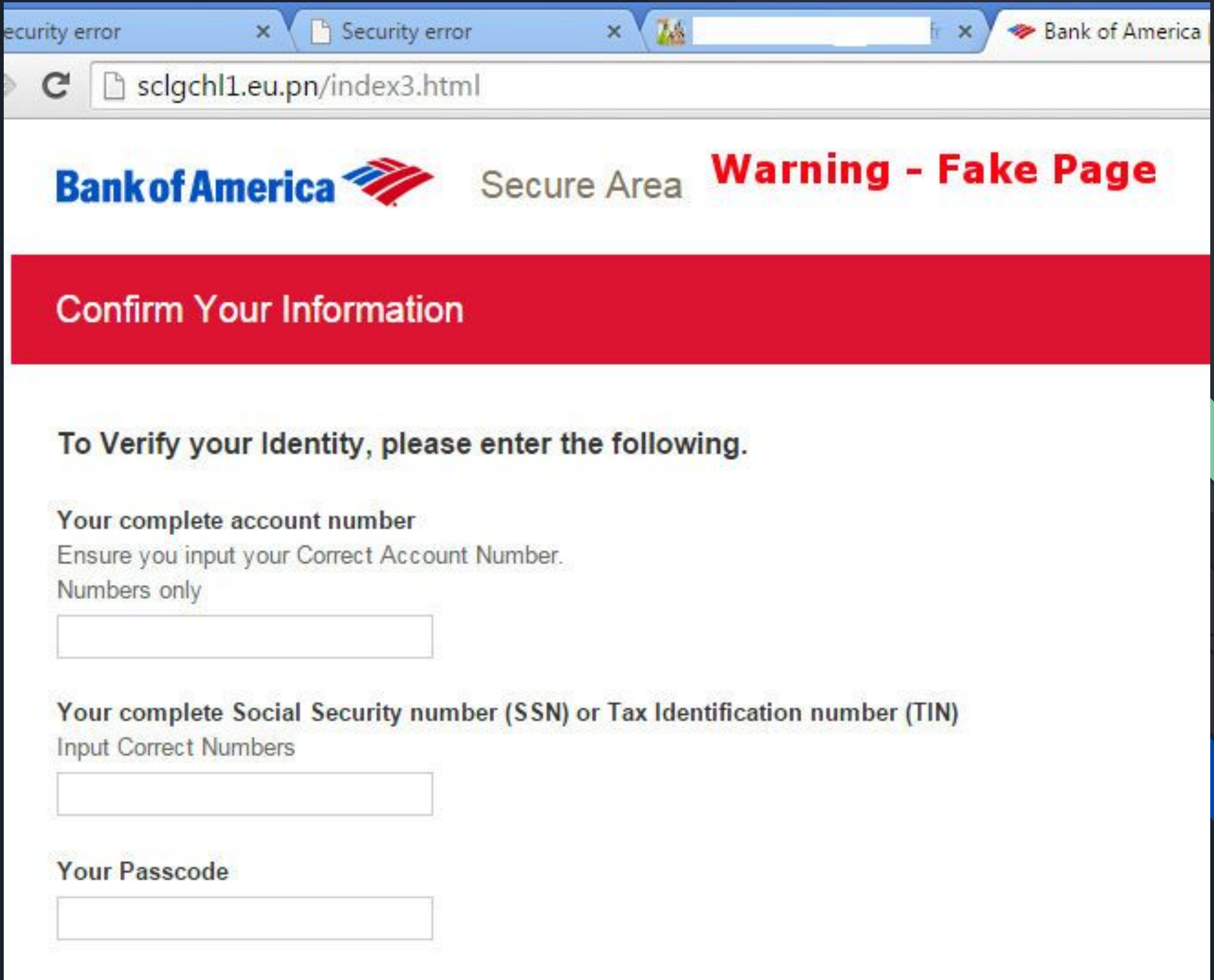
[redacted] is offline. Your messages will be sent to [redacted]'s inbox.



Text Message
Today 5:06 AM

Apple Alert

Your ICloud Is disabled due to multiple failed login attempts verify your account at http://appledevice-signin.live/ to restore full access



Bank of America Secure Area

Warning - Fake Page

Confirm Your Information

To Verify your Identity, please enter the following.

Your complete account number

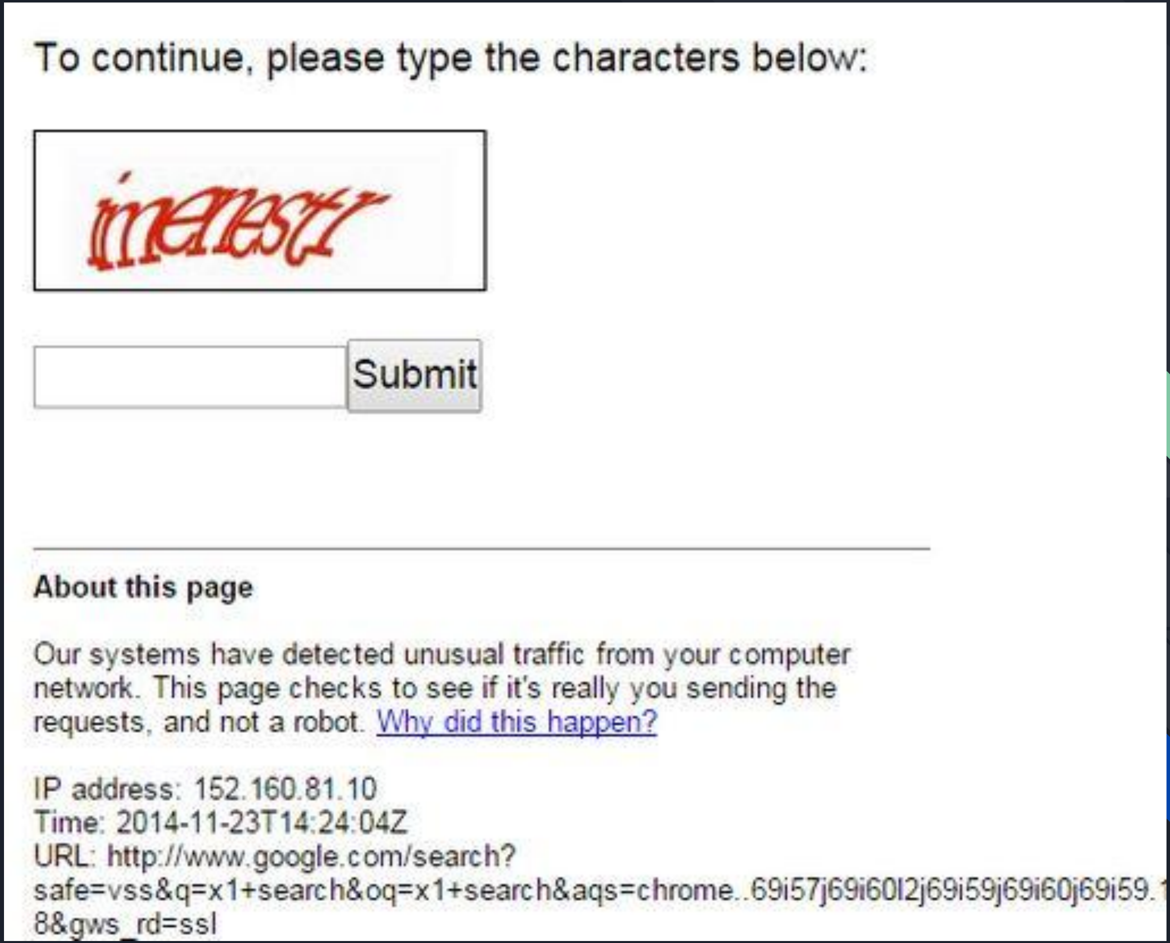
Ensure you input your Correct Account Number.

Numbers only

Your complete Social Security number (SSN) or Tax Identification number (TIN)

Input Correct Numbers

Your Passcode



To continue, please type the characters below:

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

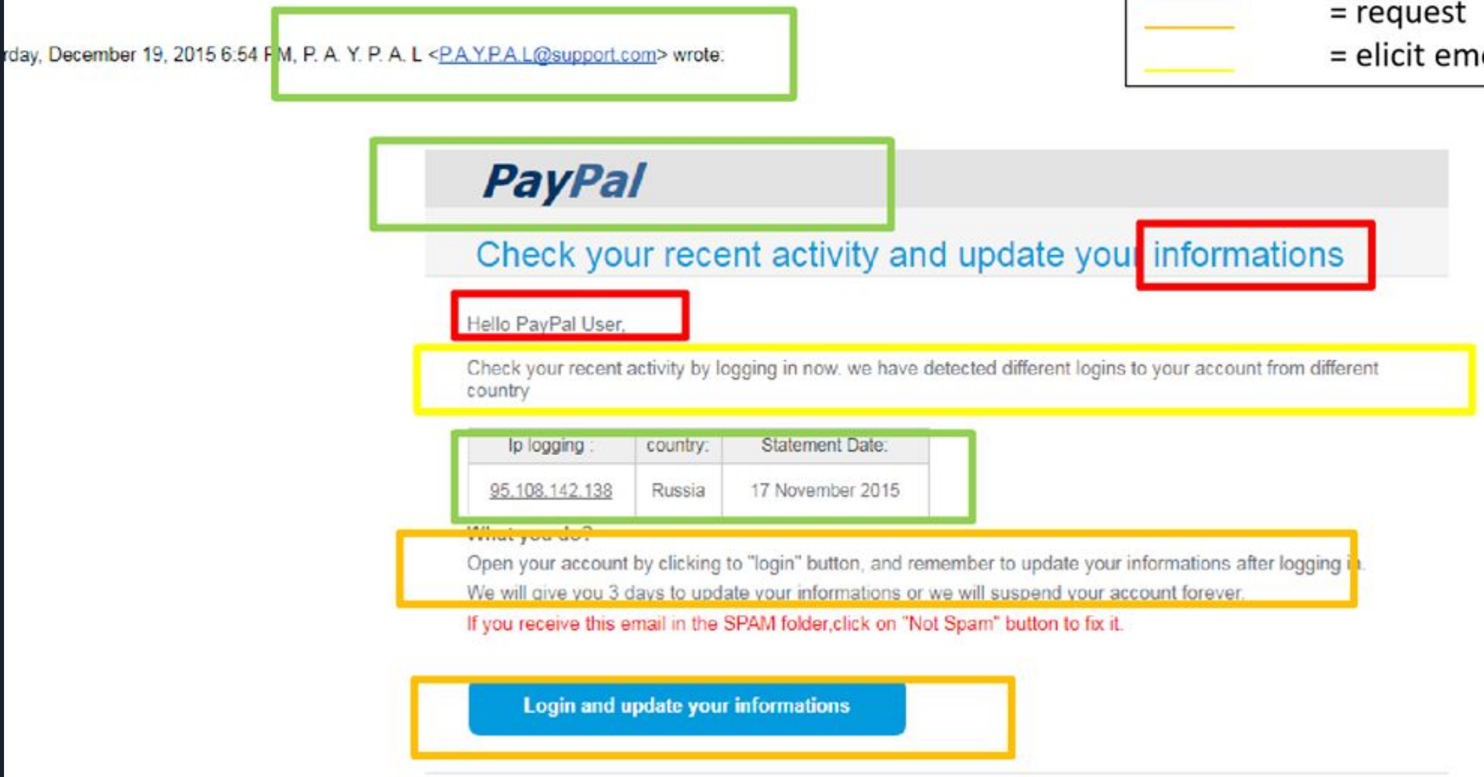
IP address: 152.160.81.10
Time: 2014-11-23T14:24:04Z
URL: http://www.google.com/search?
safe=vss&q=x1+search&oq=x1+search&aqs=chrome..69i57j69i60l2j69i59j69i60j69i59.1
8&gws_rd=ssl

🟩 = seems legitimate

🟥 = warning sign

🟧 = request

🟨 = elicit emotions



rday, December 19, 2015 6:54 PM, P. A. Y. P. A. L <P.A.Y.P.A.L@support.com> wrote:

PayPal

Check your recent activity and update your informations

Hello PayPal User,

Check your recent activity by logging in now. we have detected different logins to your account from different country

Ip logging :	country:	Statement Date:
95.108.142.138	Russia	17 November 2015

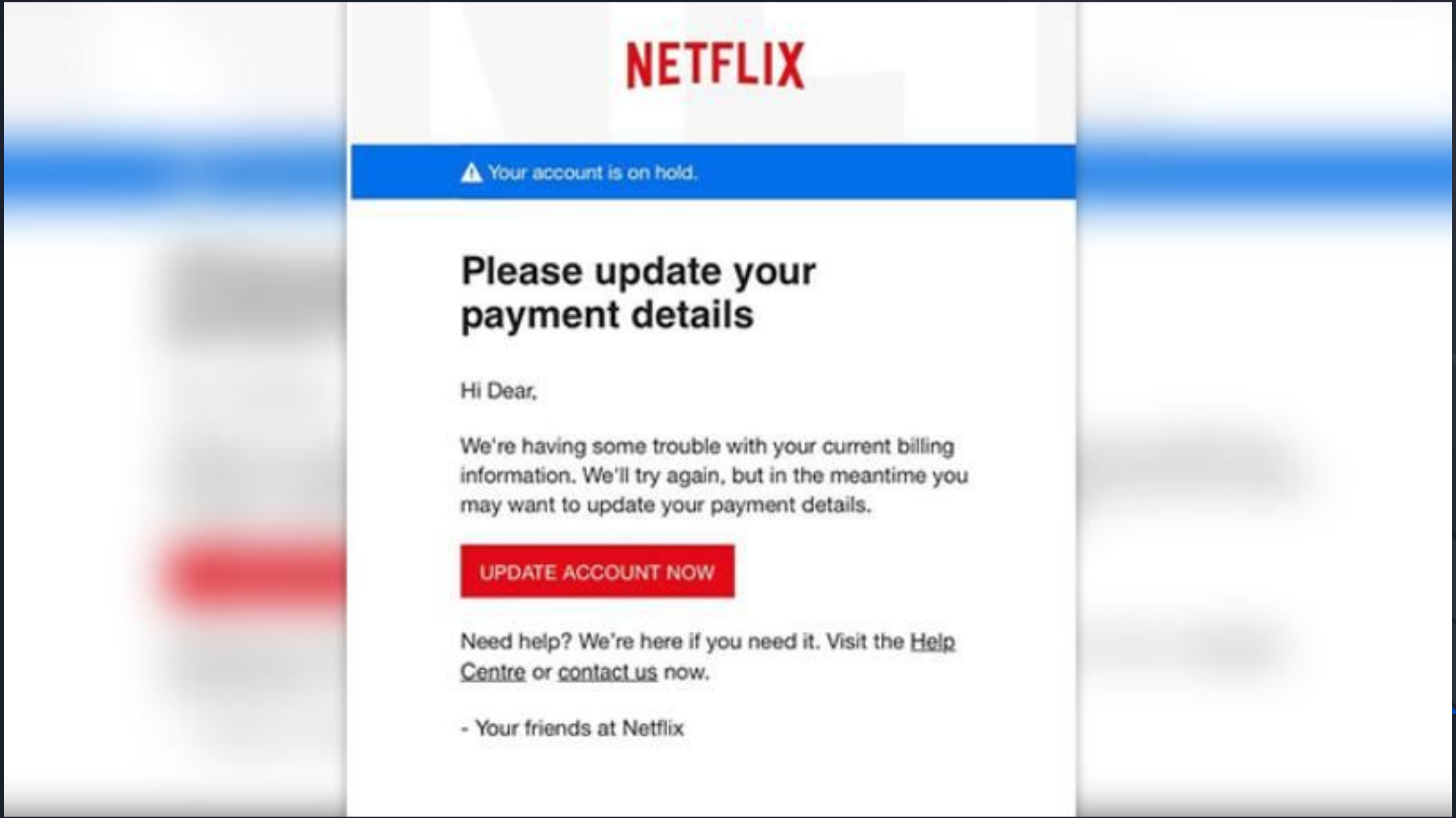
What you do?

Open your account by clicking to "login" button, and remember to update your informations after logging in.

We will give you 3 days to update your informations or we will suspend your account forever.

If you receive this email in the SPAM folder,click on "Not Spam" button to fix it.

Netflix and NOT chill!!



NETFLIX

⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

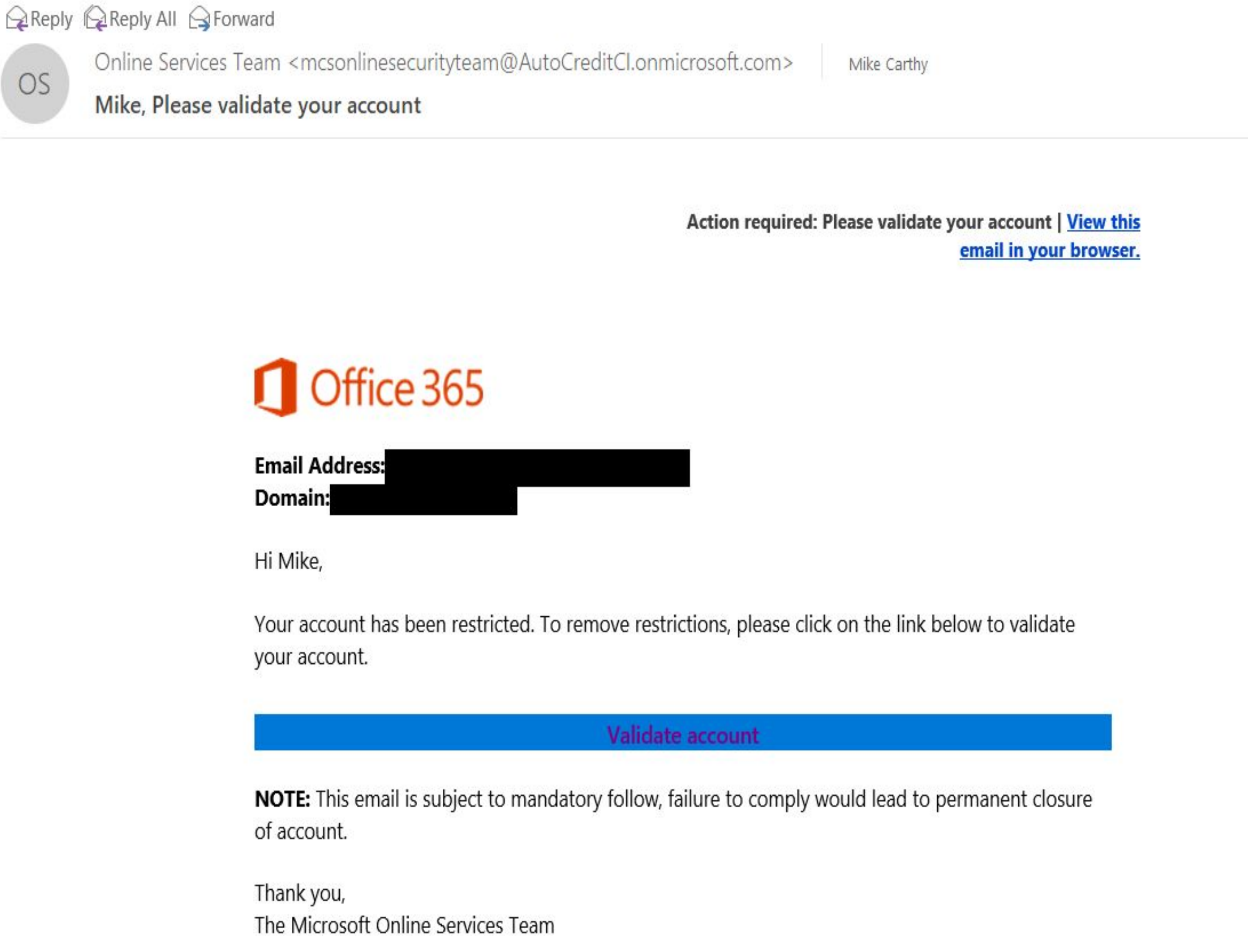
UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Sophisticated Phishing

1. Utilises DNS queries to confirm you're using O365 mail servers.
2. The HTML formatting is almost identical to a genuine Office 365 email.
3. The spelling throughout the entire email is completely accurate.
4. The email addresses “Mike” personally using their name.
5. The From address is spoofed as '**mcsonlinesecurityteam@AutoCreditCI.onmicrosoft.com**'.
6. My email address is listed at the top of the email.
7. The primary domain associated with my O365 account is also listed.
8. The phishing page looks identical to the real thing.



Online Services Team <mcsonlinesecurityteam@AutoCreditCI.onmicrosoft.com>

Mike Carthy

Mike, Please validate your account

Action required: Please validate your account | View this email in your browser.

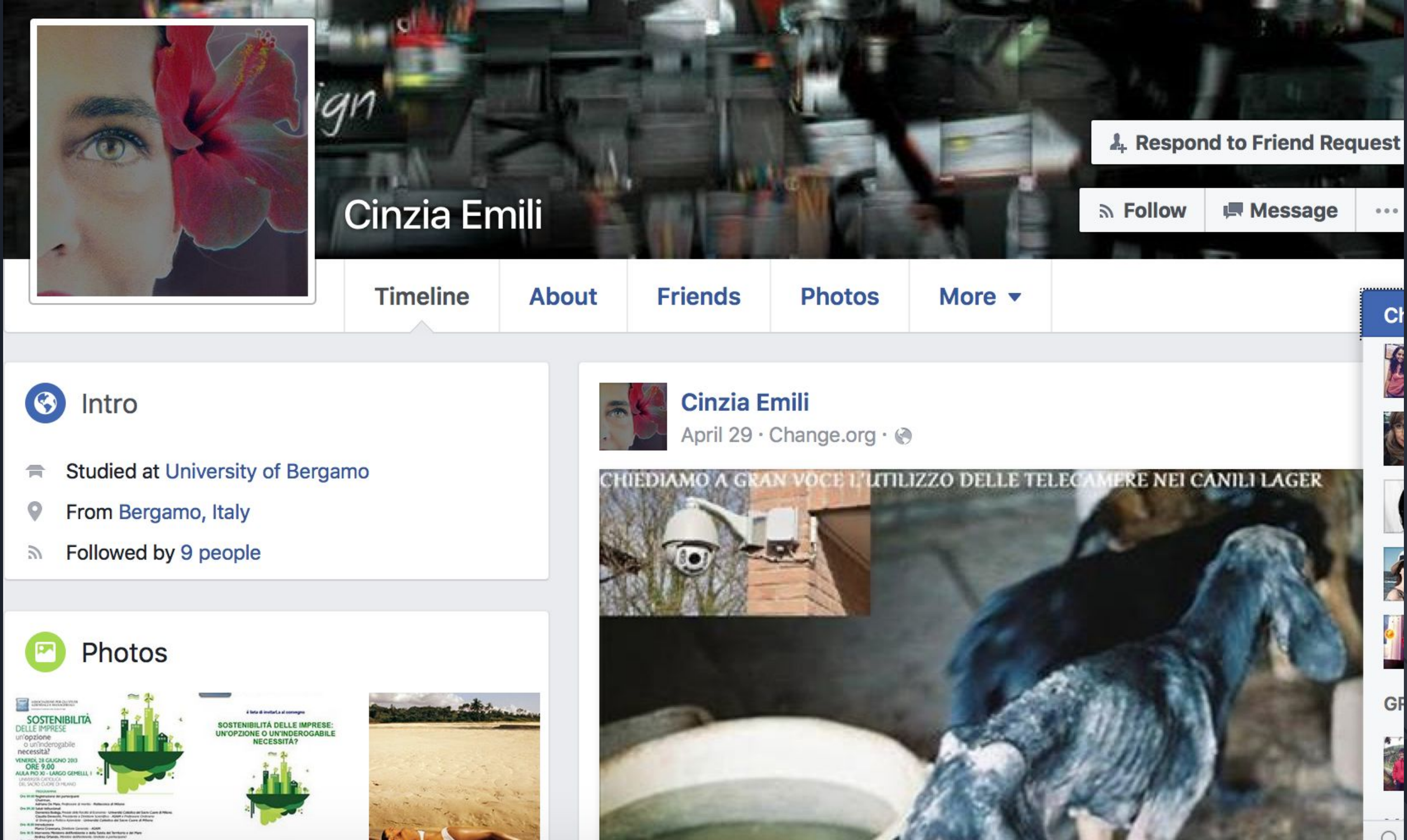
Email Address: [redacted]
Domain: [redacted]

Hi Mike,

Your account has been restricted. To remove restrictions, please click on the link below to validate your account.

NOTE: This email is subject to mandatory follow, failure to comply would lead to permanent closure of account.

Thank you,
The Microsoft Online Services Team



Respond to Friend Request
Follow
Message
Timeline
About
Friends
Photos
More

Cinzia Emili

Intro

Studied at University of Bergamo

From Bergamo, Italy

Followed by 9 people

Photos

SOSTENIBILITÀ DELLE IMPRESE un'opzione o un'inderogabile necessità?
SOSTENIBILITÀ DELLE IMPRESE: UN'OPZIONE O UN'INDEROGABILE NECESSITÀ?

Cinzia Emili

April 29 · Change.org ·

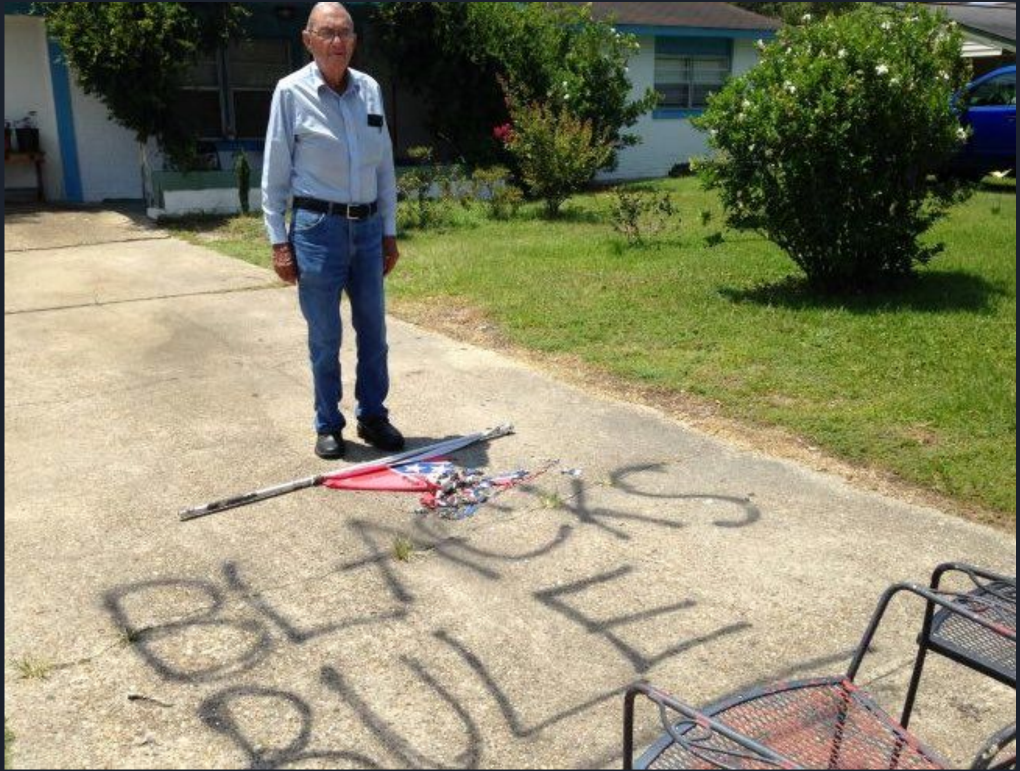
CHIEDIAMO A GRAN VOCE L'UTILIZZO DELLE TELECAMERE NEI CANILI LAGER

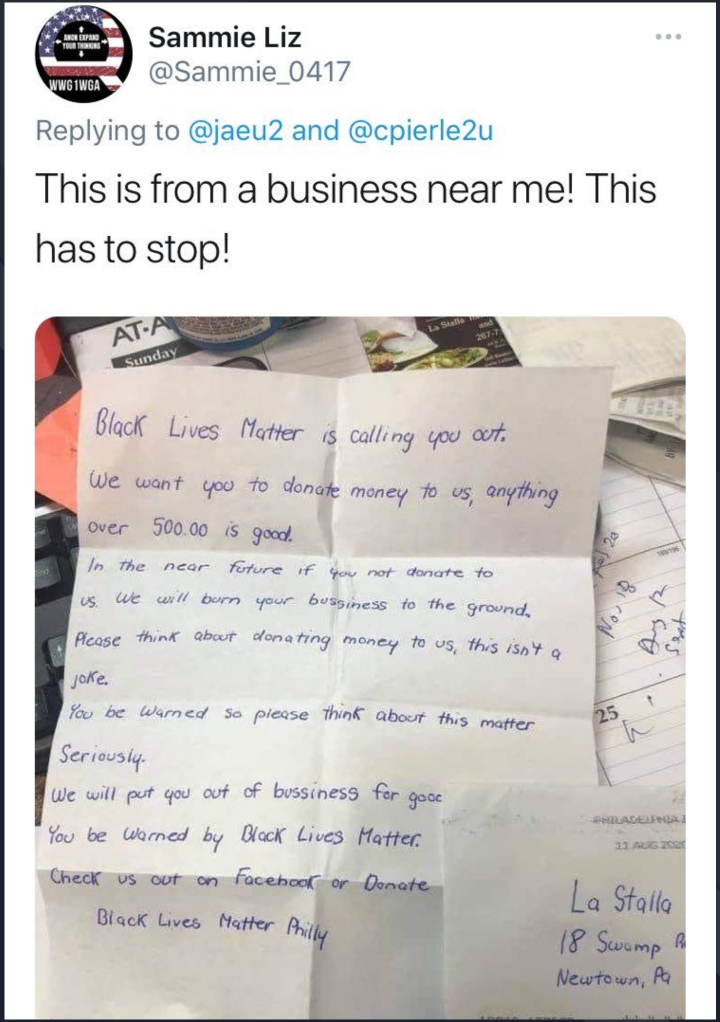
Watch out for weird looking profiles - scams or government agencies

Briefly, on disinformation.

Fear as Malware for your brain.
Where is this message coming from?
Paid ad? News organization? Was it designed to make you act on fear?

Right Wing False Flags





This is from a business near me! This has to stop!

Black Lives Matter is calling you out.

We want you to donate money to us, anything over 500.00 is good.

In the near future if you not donate to us. We will burn your bussiness to the ground.

Please think about donating money to us, this isn't a joke.

You be warned so please think about this matter Seriously.

We will put you out of bussiness for gooc

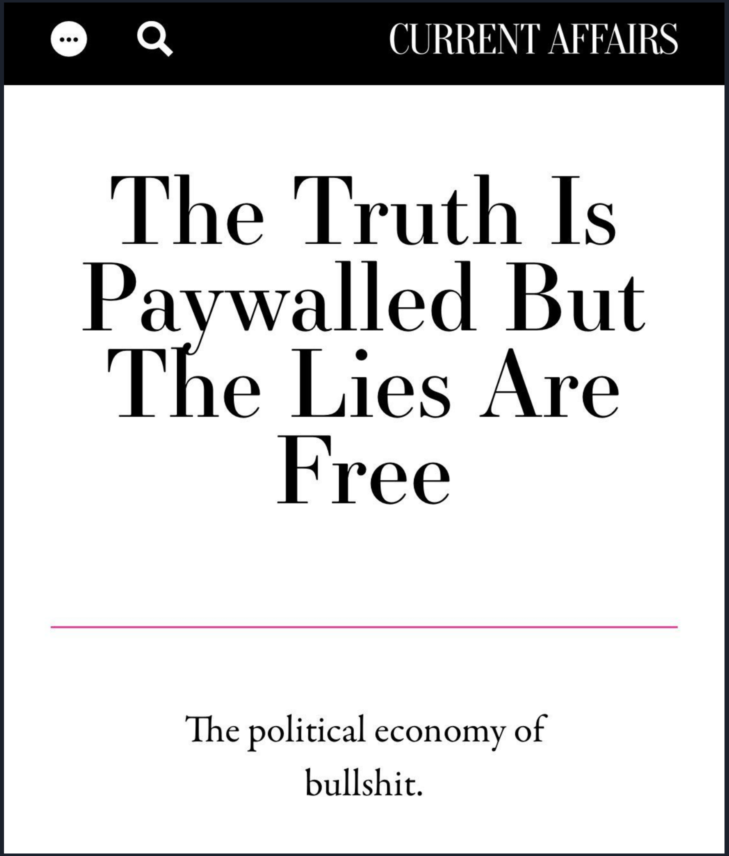
You be warned by Black Lives Matter.

Check us out on Facebook or Donate

Black Lives Matter Philly

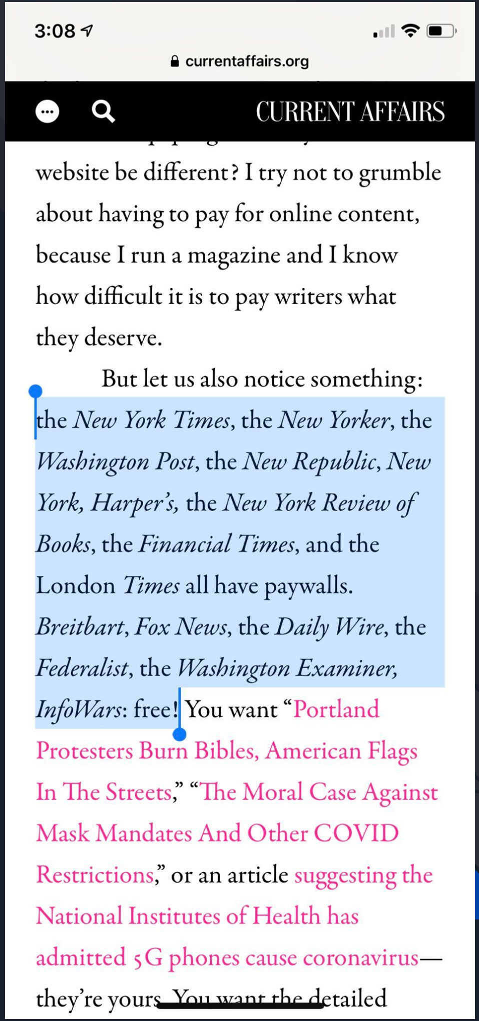
PHILADELPHIA
11 AUG 202

La Stalla
18 Swamp R
Newtown, Pa



The Truth Is Paywalled But The Lies Are Free

The political economy of bullshit.



website be different? I try not to grumble about having to pay for online content, because I run a magazine and I know how difficult it is to pay writers what they deserve.

But let us also notice something: the *New York Times*, the *New Yorker*, the *Washington Post*, the *New Republic*, *New York, Harper's,* the *New York Review of Books*, the *Financial Times*, and the London *Times* all have paywalls. *Breitbart*, *Fox News*, the *Daily Wire*, the *Federalist*, the *Washington Examiner, InfoWars*: free! You want "Portland Protesters Burn Bibles, American Flags In The Streets," "The Moral Case Against Mask Mandates And Other COVID Restrictions," or an article suggesting the National Institutes of Health has admitted 5G phones cause coronavirus—they're yours. You want the detailed

Humans, when trained and equipped with the correct knowledge, can be the strongest defense to cyber threats.

Takeaways:

Strong Passwords
Password Manager
Use a VPN
Update All Software Regularly
2FA
OpSec
Threat Modeling
E2E Everything

Questions about offensive digi sec or creating sockpuppet accounts?

PART 2:

State Sponsored Surveillance

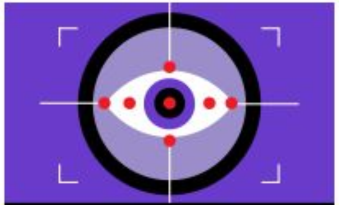
AUTOMATED LICENSE PLATE READERS (ALPRS)

BODY-WORN CAMERAS

CELL-SITE SIMULATORS/IMSI CATCHERS

FACE RECOGNITION

TATTOO RECOGNITION



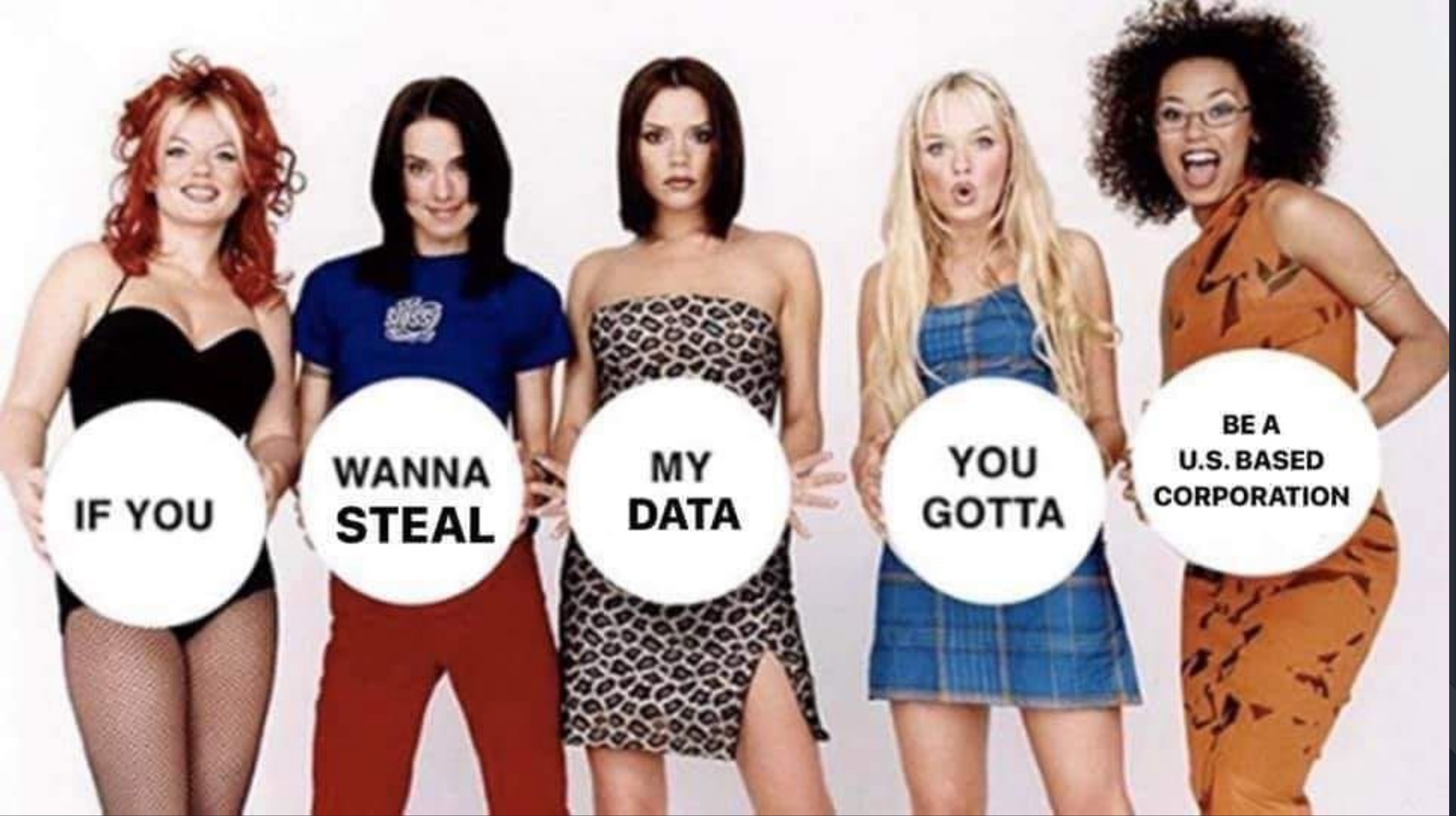
IRIS RECOGNITION

SECURITY CAMERAS

DRONES/UNMANNED AERIAL VEHICLES

ELECTRONIC MONITORING

GUNSHOT DETECTION

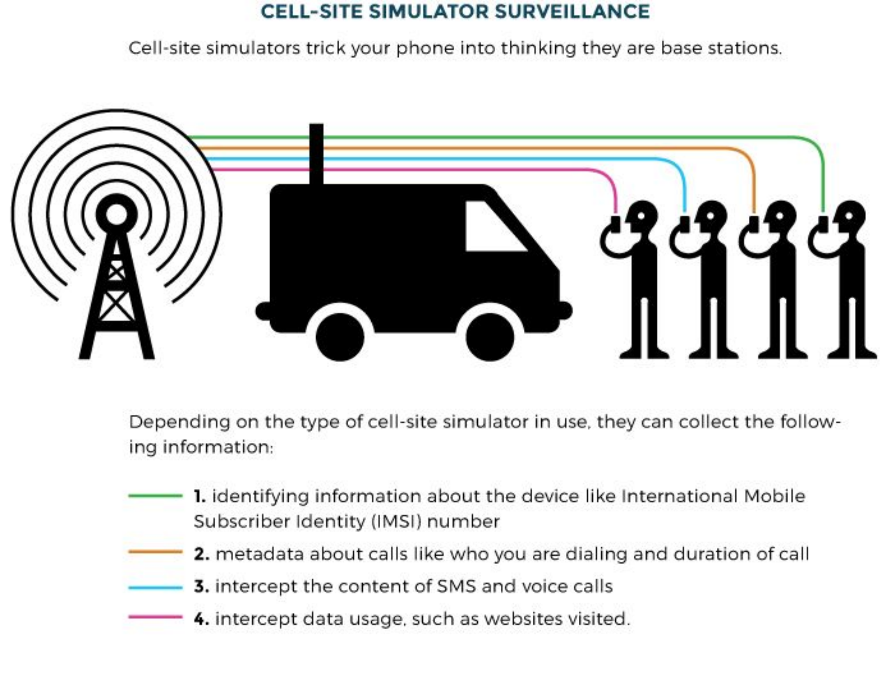

IF YOU
WANNA STEAL
MY DATA
YOU GOTTA
BE A U.S. BASED CORPORATION

https://ir.netscout.com/investors/press-releases/press-release-details/2003/Oregons-TriMet-Uses-NetScout-to-Monitor-Networked-Transit-Security------------------------------and-GPS-Tracking-Systems/default.aspx

https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

https://hackaday.com/2016/08/09/how-to-detect-and-find-rogue-cell-towers/

Cellphone Tower Emulator

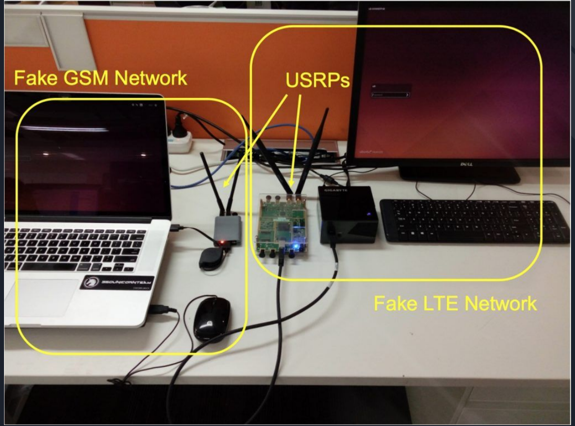


CELL-SITE SIMULATOR SURVEILLANCE

Cell-site simulators trick your phone into thinking they are base stations.

Depending on the type of cell-site simulator in use, they can collect the following information:

1. identifying information about the device like International Mobile Subscriber Identity (IMSI) number
2. metadata about calls like who you are dialing and duration of call
3. intercept the content of SMS and voice calls
4. intercept data usage, such as websites visited.



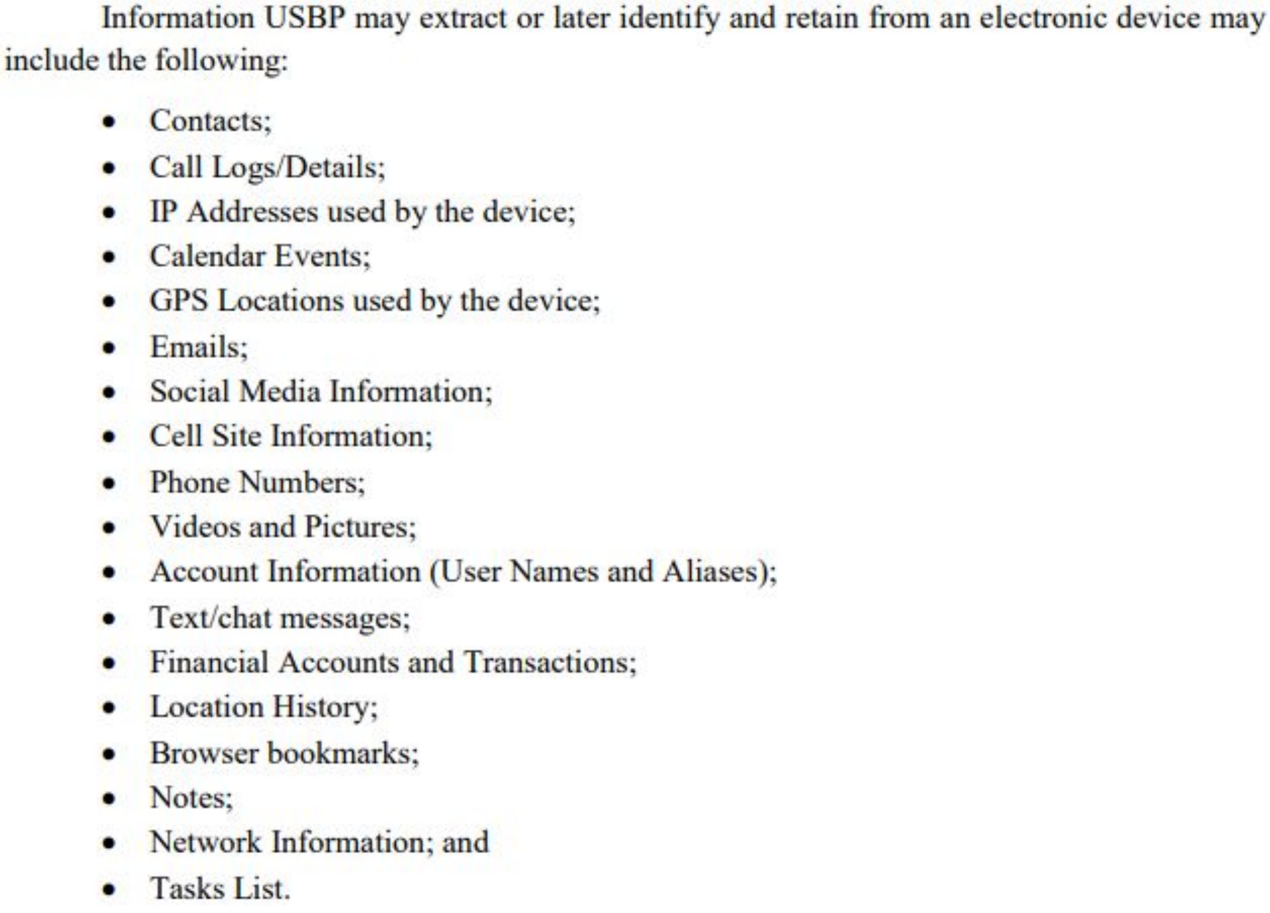
Stingray Detection and Prevention

Some indications of possible cellphone surveillance occurring may include a mobile phone waking up unexpectedly, using a lot of the CPU when on idle or when not in use, hearing clicking or beeping sounds when conversations are occurring and the circuit board of the phone being warm despite the phone not being used.

Preventive measures against cellphone surveillance include not losing or allowing strangers to use a mobile phone and the utilization of an access password. Turning off and then also removing the battery from a phone when not in use is another technique.A Faraday cage may also work.

Silent Pocket®
2015 Silent Pocket® is a brand of Peeled Group LLC
All rights reserved · Designed in Encinitas, CA ·

With your phone or computer, CBP can access:

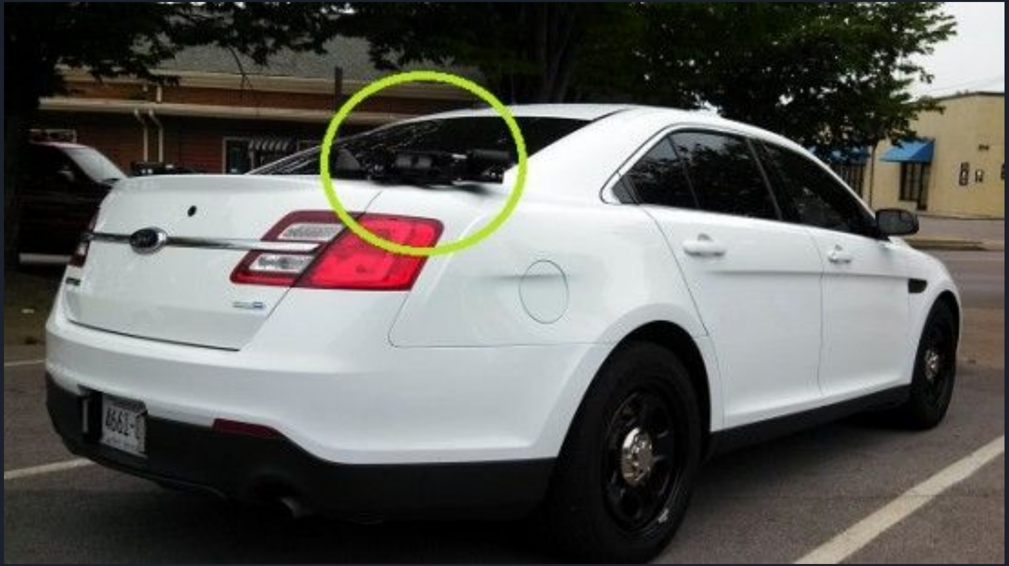


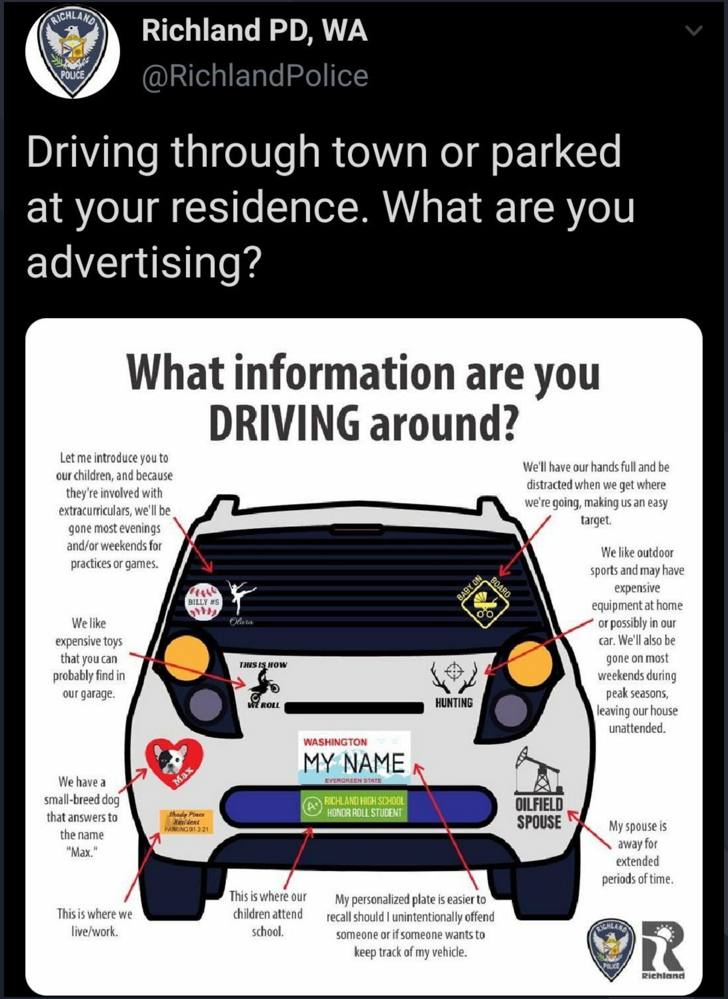
Information USBP may extract or later identify and retain from an electronic device may include the following:

- Contacts;
- Call Logs/Details;
- IP Addresses used by the device;
- Calendar Events;
- GPS Locations used by the device;
- Emails;
- Social Media Information;
- Cell Site Information;
- Phone Numbers;
- Videos and Pictures;
- Account Information (User Names and Aliases);
- Text/chat messages;
- Financial Accounts and Transactions;
- Location History;
- Browser bookmarks;
- Notes;
- Network Information; and
- Tasks List.

https://www.cnet.com/news/license-plate-tracking-for-police-set-to-go-nationwide/

APLRs





Richland PD, WA
@RichlandPolice

Driving through town or parked at your residence. What are you advertising?

What information are you DRIVING around?

Let me introduce you to our children, and because they're involved with extracurriculars, we'll be gone most evenings and/or weekends for practices or games.

We like expensive toys that you can probably find in our garage.

We have a small-breed dog that answers to the name "Max."

This is where we live/work.

We'll have our hands full and be distracted when we get where we're going, making us an easy target.

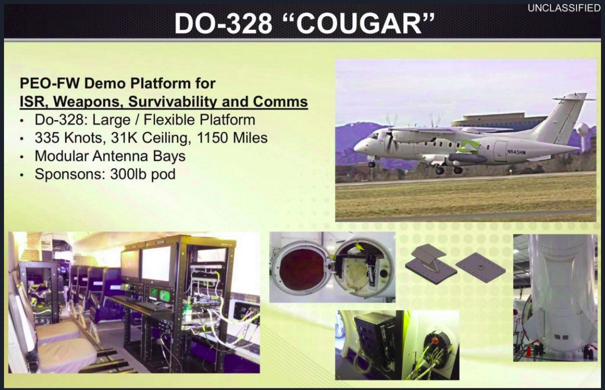
We like outdoor sports and may have expensive equipment at home or possibly in our car. We'll also be gone on most weekends during peak seasons, leaving our house unattended.

My spouse is away for extended periods of time.

This is where our children attend school.

My personalized plate is easier to recall should I unintentionally offend someone or if someone wants to keep track of my vehicle.

Aerial Surveillance

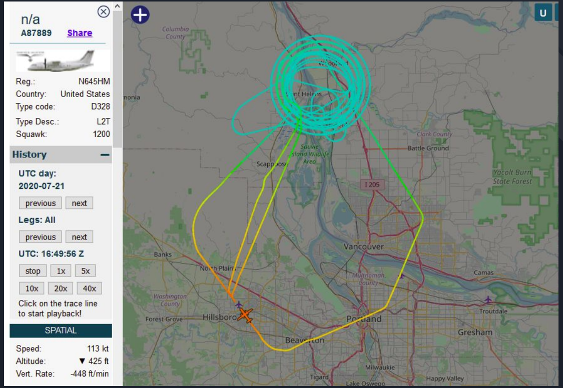


UNCLASSIFIED

DO-328 "COUGAR"

PEO-FW Demo Platform for
ISR, Weapons, Survivability and Comms

- Do-328: Large / Flexible Platform
- 335 Knots, 31K Ceiling, 1150 Miles
- Modular Antenna Bays
- Sponsons: 300lb pod



n/a
A87889 Share

Reg.: N645HM
Country: United States
Type code: D328
Type Desc.: L2T
Squawk: 1200

History –

UTC day: 2020-07-21

previous next

Legs: All

previous next

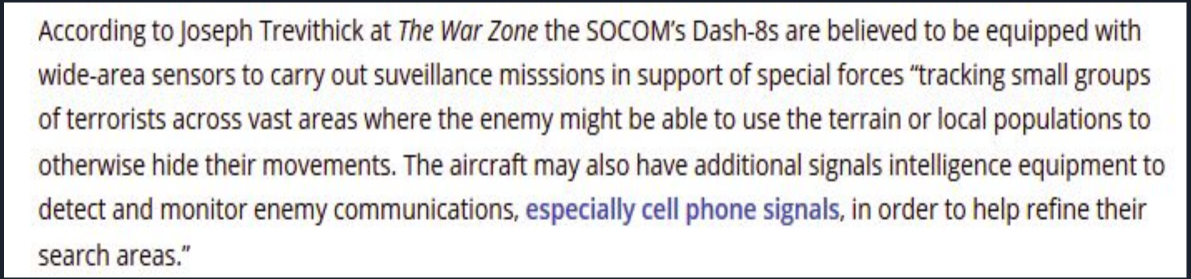
UTC: 16:49:56 Z

stop 1x 5x
10x 20x 40x

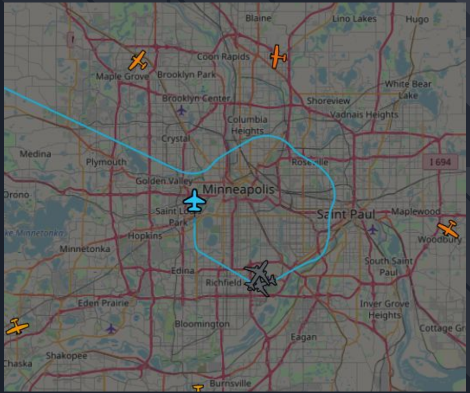
Click on the trace line to start playback!

SPATIAL

Speed: 113 kt
Altitude: ▼ 425 ft
Vert. Rate: -448 ft/min



According to Joseph Trevithick at *The War Zone* the SOCOM's Dash-8s are believed to be equipped with wide-area sensors to carry out suveillance misssions in support of special forces "tracking small groups of terrorists across vast areas where the enemy might be able to use the terrain or local populations to otherwise hide their movements. The aircraft may also have additional signals intelligence equipment to detect and monitor enemy communications, especially cell phone signals, in order to help refine their search areas."



U.S. Customs and Border Protection

Unmanned Aircraft System MQ-9 Predator B

FACT SHEET

U.S. Customs and Border Protection's (CBP) Air and Marine Operations (AMO) operates the highly capable and proven Predator B unmanned aircraft system (UAS) to further enhance operational capabilities and increase domain awareness. AMO selected the Predator B, manufactured by General Atomics Aeronautical Systems, for its unique combination of operational capabilities, payload capacity, mission flexibility, potential to accommodate new sensor packages, and its safety and performance record with other federal agencies.

The UAS program focuses operations on the CBP priority mission of anti-terrorism by helping to identify and intercept potential terrorists and illegal cross-border activity.

AMO also deploys the UAS to aid in disaster relief and emergency response efforts of its Department of Homeland Security partners, including the Federal Emergency Management Agency and the U.S. Coast Guard.

The remotely-piloted Predator B allows AMO personnel to safely conduct missions in areas that are difficult to access or otherwise too high-risk for manned aircraft or CBP ground personnel.

AMO first employed the Predator B to enhance law enforcement operations on the Southwest Border in 2005 and along the Northern Border in 2009. AMO has operated Predator Bs from Libby Army Airfield in Sierra Vista, Arizona, and along the Texas border since 2011.

AMO also operates a maritime variant UAS called the Guardian. AMO's Guardian aircraft fly from Naval Air Station Corpus Christi in Texas and along the Northern Region. The Guardian can be operated from any designated UAS location to conduct missions within the maritime border areas. AMO expects to employ the Predator B throughout the border regions with command and control from a network of ground control stations across the country. The Predator B's capability to provide high-quality streaming video to first responders, and to assess critical infrastructure before and after events, makes it an ideal aircraft to aid in emergency preparations and recovery operations.

The UAS has provided emergency support for multiple hurricanes and floods since 2008. Video recorders document suspect activities for evidentiary use.

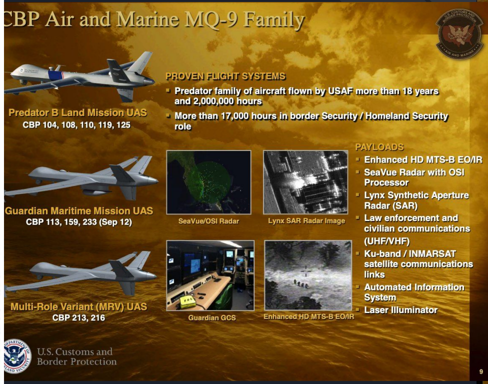
Performance and Weight:

- **Maximum Speed**
  240 knots (276 mph)
- **Service Ceiling Altitude**
  50,000 feet
- **Endurance**
  Up to 20 hours
- **Maximum Gross Weight**
  10,500 pounds

Other System Components

- Fixed and mobile ground control stations
- Electro-optical/infrared sensors, which allow for crewmembers to maintain awareness of targets in all environments
- Surface search radar/ground moving target indicator

For more information, visit the CBP.gov website
or contact the Office of Public Affairs at (202) 344-1780.



CBP Air and Marine MQ-9 Family

Predator B Land Mission UAS
CBP 104, 108, 110, 119, 125

Guardian Maritime Mission UAS
CBP 113, 159, 233 (Sep 12)

Multi-Role Variant (MRV) UAS
CBP 213, 216

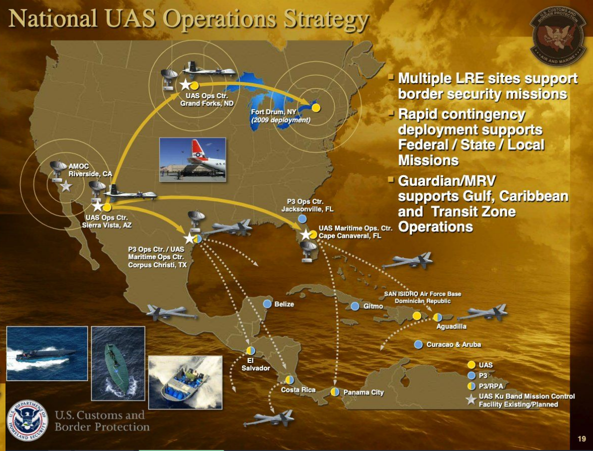
PROVEN FLIGHT SYSTEMS

- Predator family of aircraft flown by USAF more than 18 years and 2,000,000 hours
- More than 17,000 hours in border Security / Homeland Security role

PAYLOADS

- Enhanced HD MTS-B EO/IR
- SeaVue Radar with OSI Processor
- Lynx Synthetic Aperture Radar (SAR)
- Law enforcement and civilian communications (UHF/VHF)
- Ku-band / INMARSAT satellite communications links
- Automated Information System
- Laser Illuminator

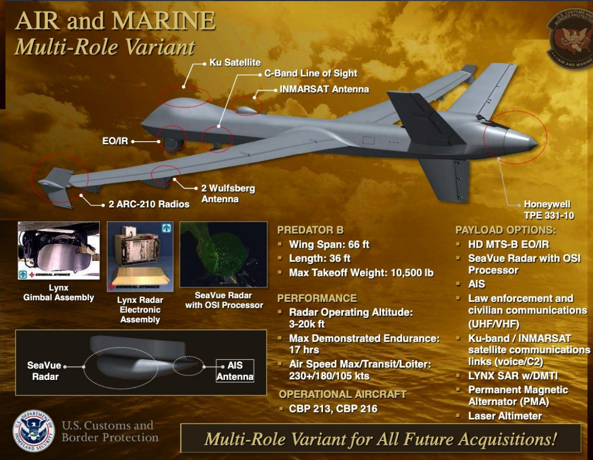
U.S. Customs and Border Protection



National UAS Operations Strategy

- Multiple LRE sites support border security missions
- Rapid contingency deployment supports Federal / State / Local Missions
- Guardian/MRV supports Gulf, Caribbean and Transit Zone Operations

U.S. Customs and Border Protection



AIR and MARINE
Multi-Role Variant

PREDATOR B

- Wing Span: 66 ft
- Length: 36 ft
- Max Takeoff Weight: 10,500 lb

PERFORMANCE

- Radar Operating Altitude: 3-20k ft
- Max Demonstrated Endurance: 17 hrs
- Air Speed Max/Transit/Loiter: 230+/180/105 kts

OPERATIONAL AIRCRAFT

- CBP 213, CBP 216

PAYLOAD OPTIONS:

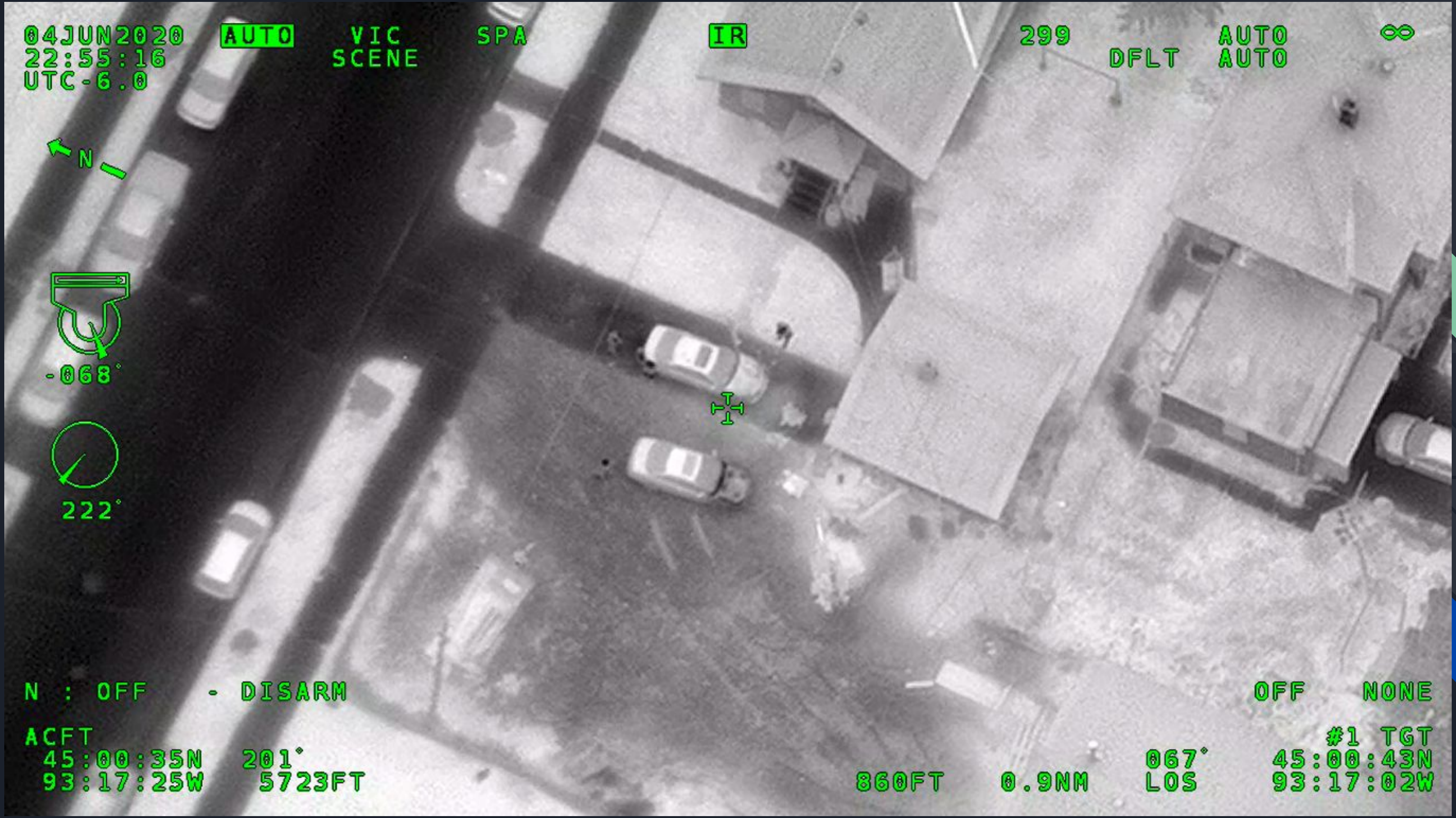
- HD MTS-B EO/IR
- SeaVue Radar with OSI Processor
- AIS
- Law enforcement and civilian communications (UHF/VHF)
- Ku-band / INMARSAT satellite communications links (voice/C2)
- LYNX SAR w/DMTI
- Permanent Magnetic Alternator (PMA)
- Laser Altimeter

U.S. Customs and Border Protection

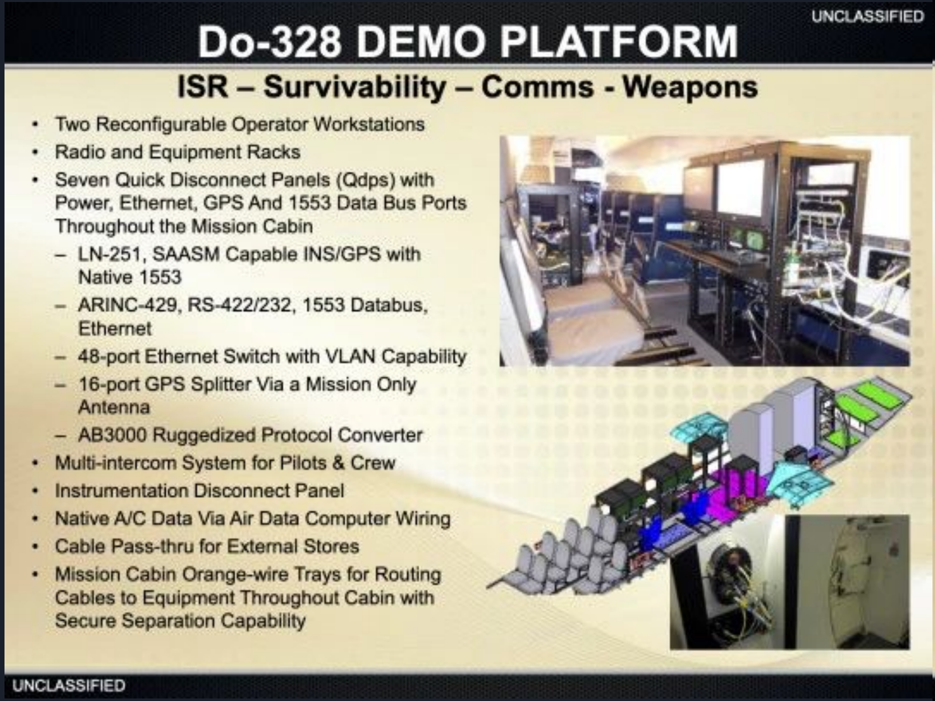
Multi-Role Variant for All Future Acquisitions!

Police Drones

DHS Cessnas Thermal Camera View



Air Force Surveillance DO-328 “Cougar”



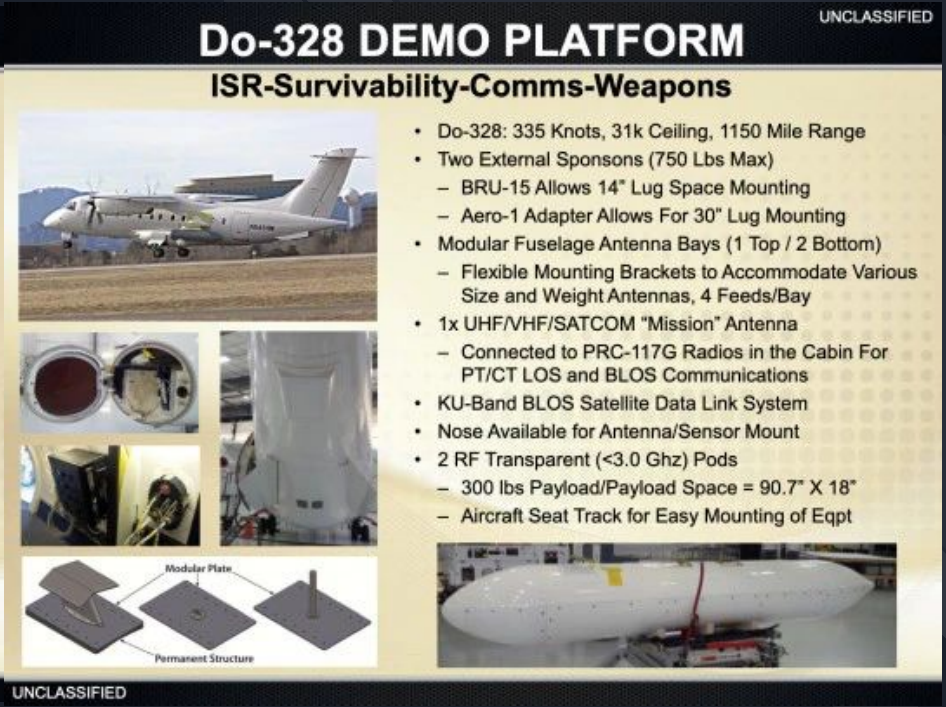
UNCLASSIFIED

Do-328 DEMO PLATFORM

ISR – Survivability – Comms - Weapons

- Two Reconfigurable Operator Workstations
- Radio and Equipment Racks
- Seven Quick Disconnect Panels (Qdps) with Power, Ethernet, GPS And 1553 Data Bus Ports Throughout the Mission Cabin
  - LN-251, SAASM Capable INS/GPS with Native 1553
  - ARINC-429, RS-422/232, 1553 Databus, Ethernet
  - 48-port Ethernet Switch with VLAN Capability
  - 16-port GPS Splitter Via a Mission Only Antenna
  - AB3000 Ruggedized Protocol Converter
- Multi-intercom System for Pilots & Crew
- Instrumentation Disconnect Panel
- Native A/C Data Via Air Data Computer Wiring
- Cable Pass-thru for External Stores
- Mission Cabin Orange-wire Trays for Routing Cables to Equipment Throughout Cabin with Secure Separation Capability

UNCLASSIFIED



UNCLASSIFIED

Do-328 DEMO PLATFORM

ISR-Survivability-Comms-Weapons

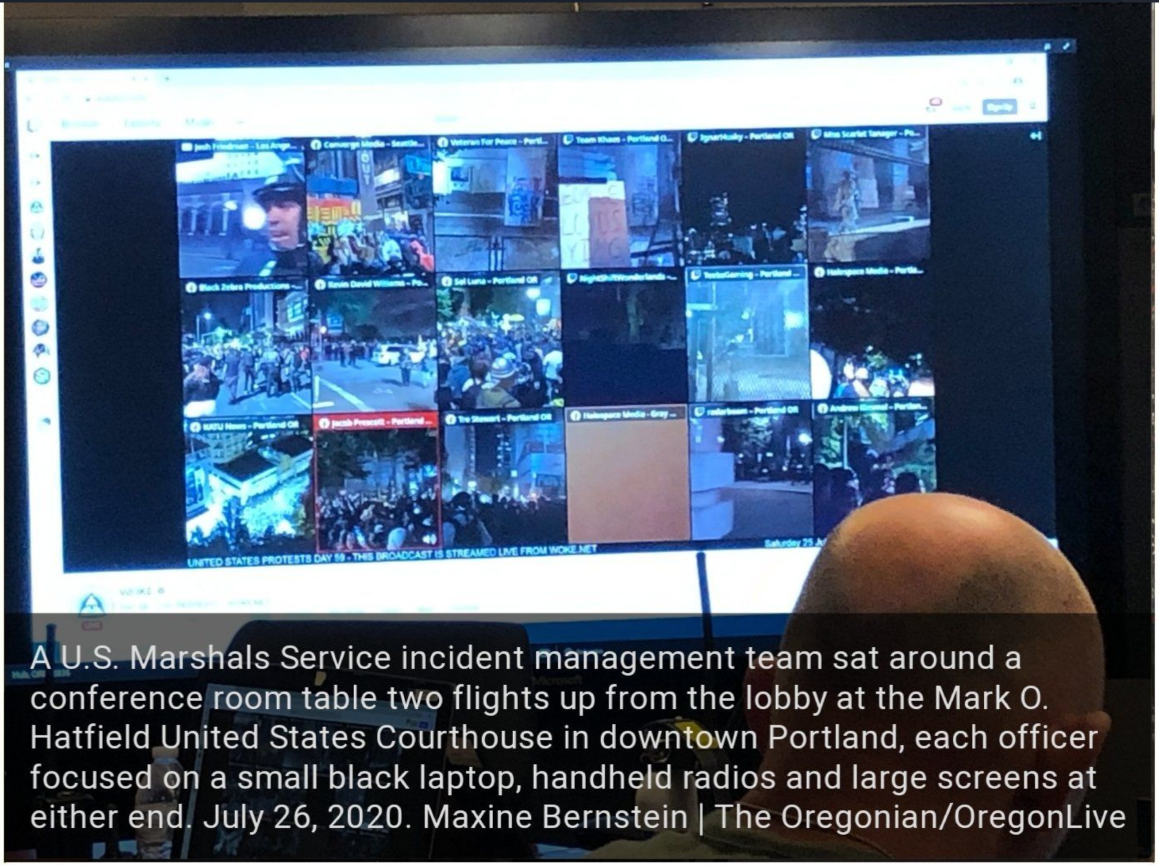
- Do-328: 335 Knots, 31k Ceiling, 1150 Mile Range
- Two External Sponsons (750 Lbs Max)
  - BRU-15 Allows 14" Lug Space Mounting
  - Aero-1 Adapter Allows For 30" Lug Mounting
- Modular Fuselage Antenna Bays (1 Top / 2 Bottom)
  - Flexible Mounting Brackets to Accommodate Various Size and Weight Antennas, 4 Feeds/Bay
- 1x UHF/VHF/SATCOM “Mission” Antenna
  - Connected to PRC-117G Radios in the Cabin For PT/CT LOS and BLOS Communications
- KU-Band BLOS Satellite Data Link System
- Nose Available for Antenna/Sensor Mount
- 2 RF Transparent (<3.0 Ghz) Pods
  - 300 lbs Payload/Payload Space = 90.7" X 18"
  - Aircraft Seat Track for Easy Mounting of Eqpt

UNCLASSIFIED

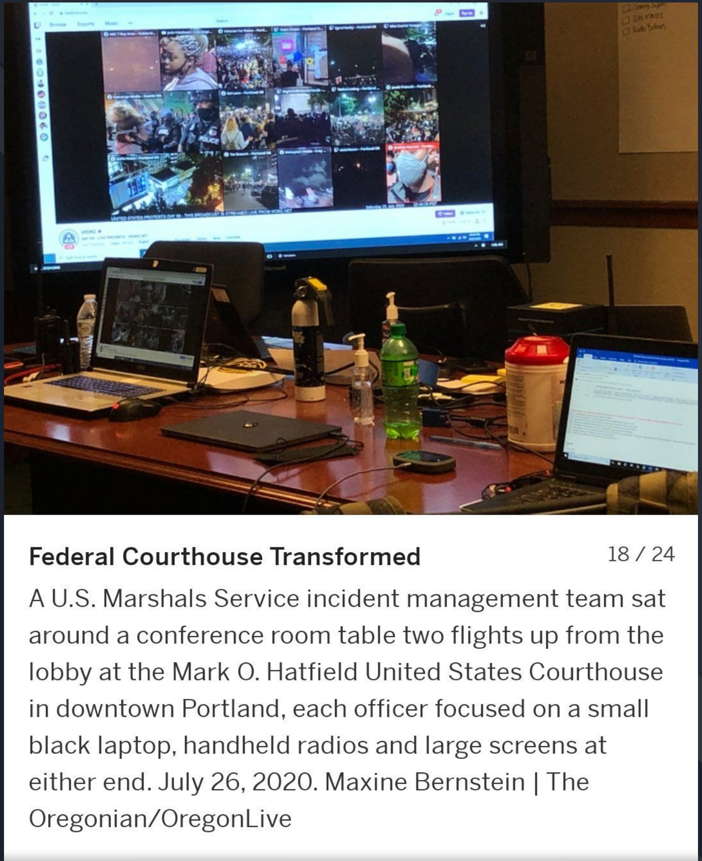
Social Media Surveillance

https://www.thenation.com/article/archive/the-fbi-is-setting-up-a-task-force-to-monitor-social-media/

US Marshals Monitoring Protest Livestreams


UNITED STATES PROTESTS DAY 59 - THIS BROADCAST IS STREAMED LIVE FROM WOKE.NET

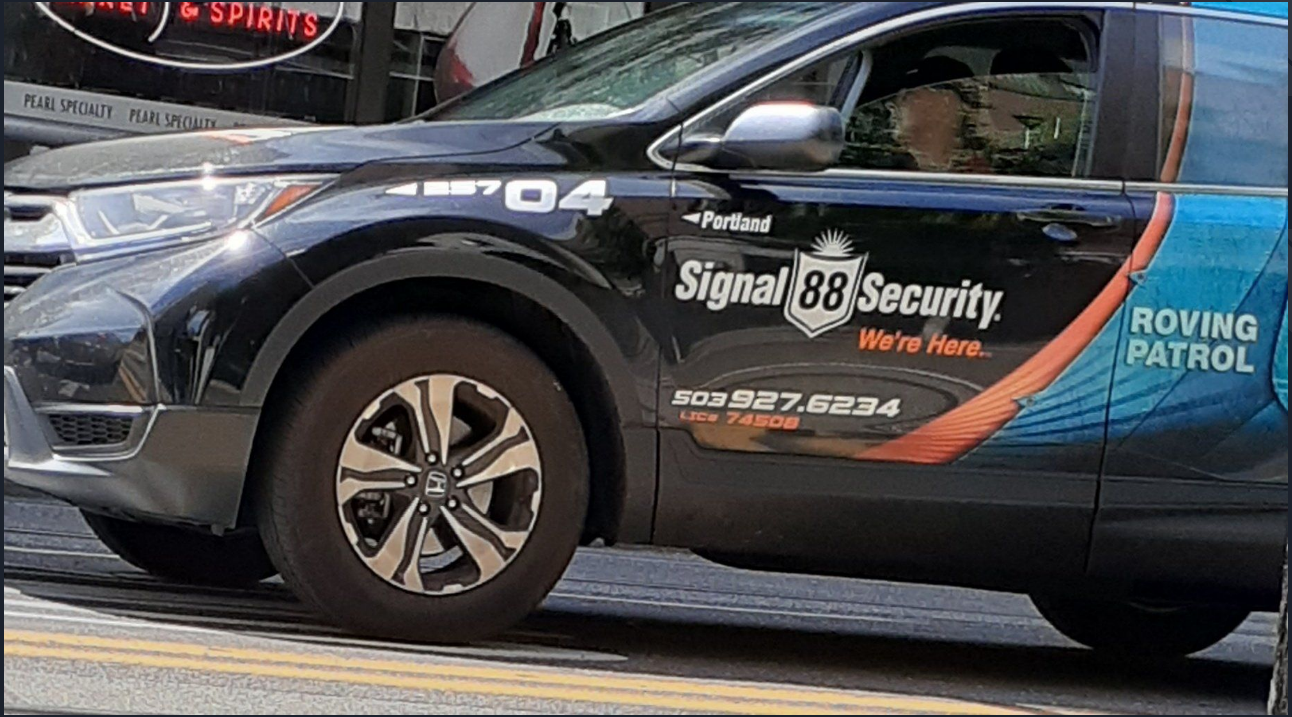
A U.S. Marshals Service incident management team sat around a conference room table two flights up from the lobby at the Mark O. Hatfield United States Courthouse in downtown Portland, each officer focused on a small black laptop, handheld radios and large screens at either end. July 26, 2020. Maxine Bernstein | The Oregonian/OregonLive



Federal Courthouse Transformed 18 / 24

A U.S. Marshals Service incident management team sat around a conference room table two flights up from the lobby at the Mark O. Hatfield United States Courthouse in downtown Portland, each officer focused on a small black laptop, handheld radios and large screens at either end. July 26, 2020. Maxine Bernstein | The Oregonian/OregonLive

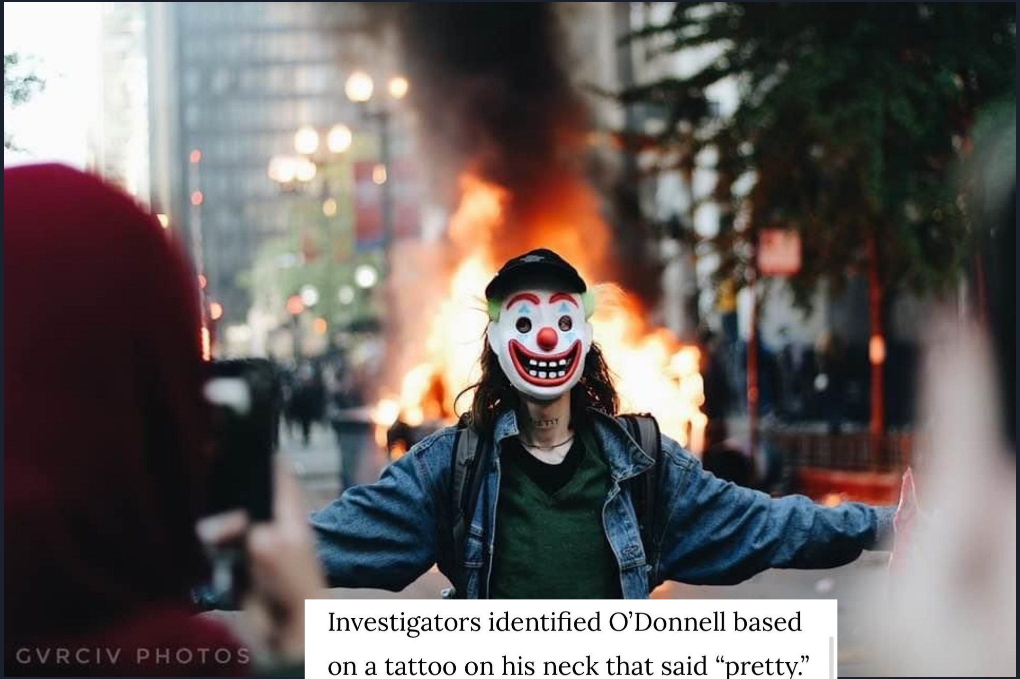
Private Police aka Private Security



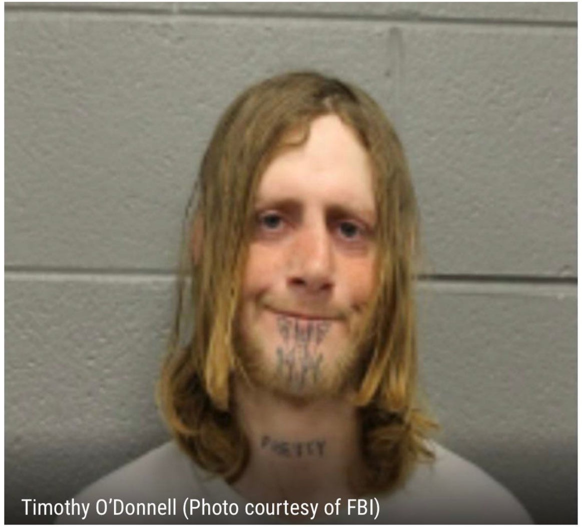
Facial Recognition

https://whohasyourface.org/

Tattoos as Identifiers



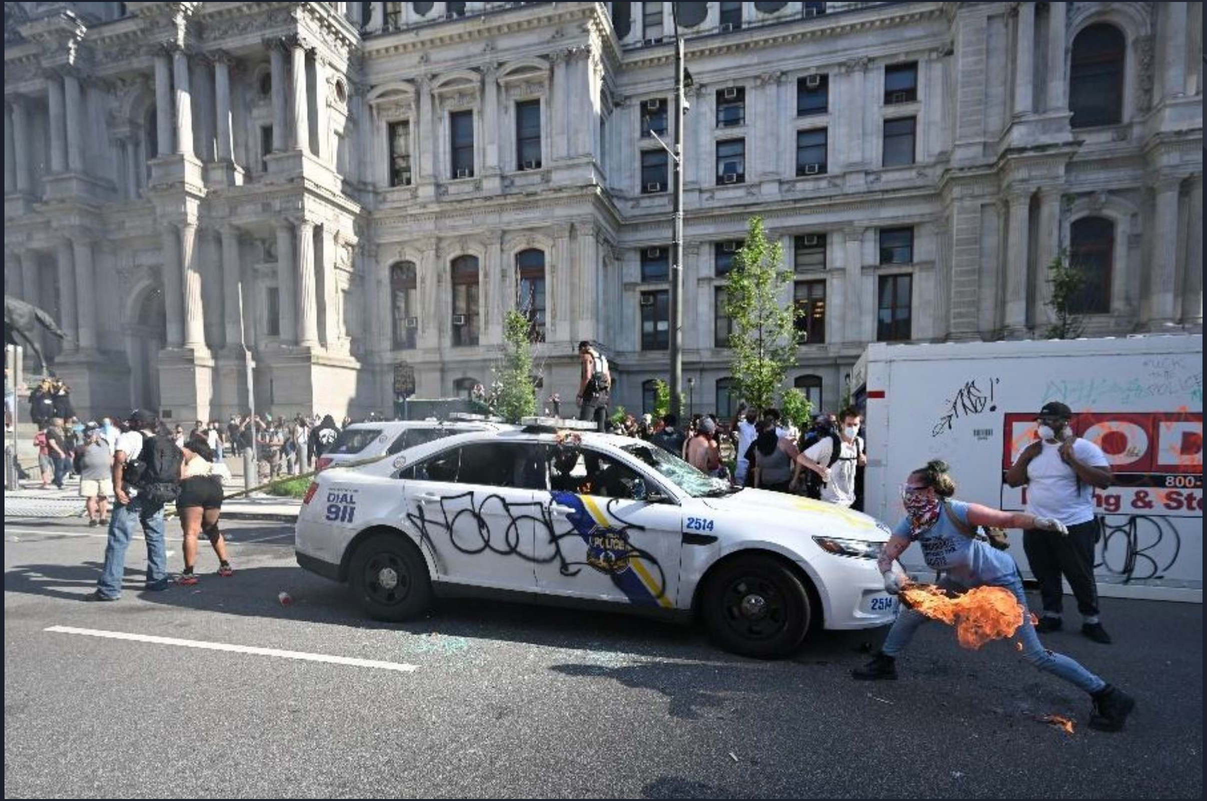
Investigators identified O’Donnell based on a tattoo on his neck that said “pretty.” He was arrested Tuesday at his apartment on 19th Place in Pilsen.


Timothy O’Donnell (Photo courtesy of FBI)

CHICAGO — A Chicago man is facing federal arson charges after investigators said he set fire to a Chicago police squad car.

Lore Elisabeth Blumenthal Case

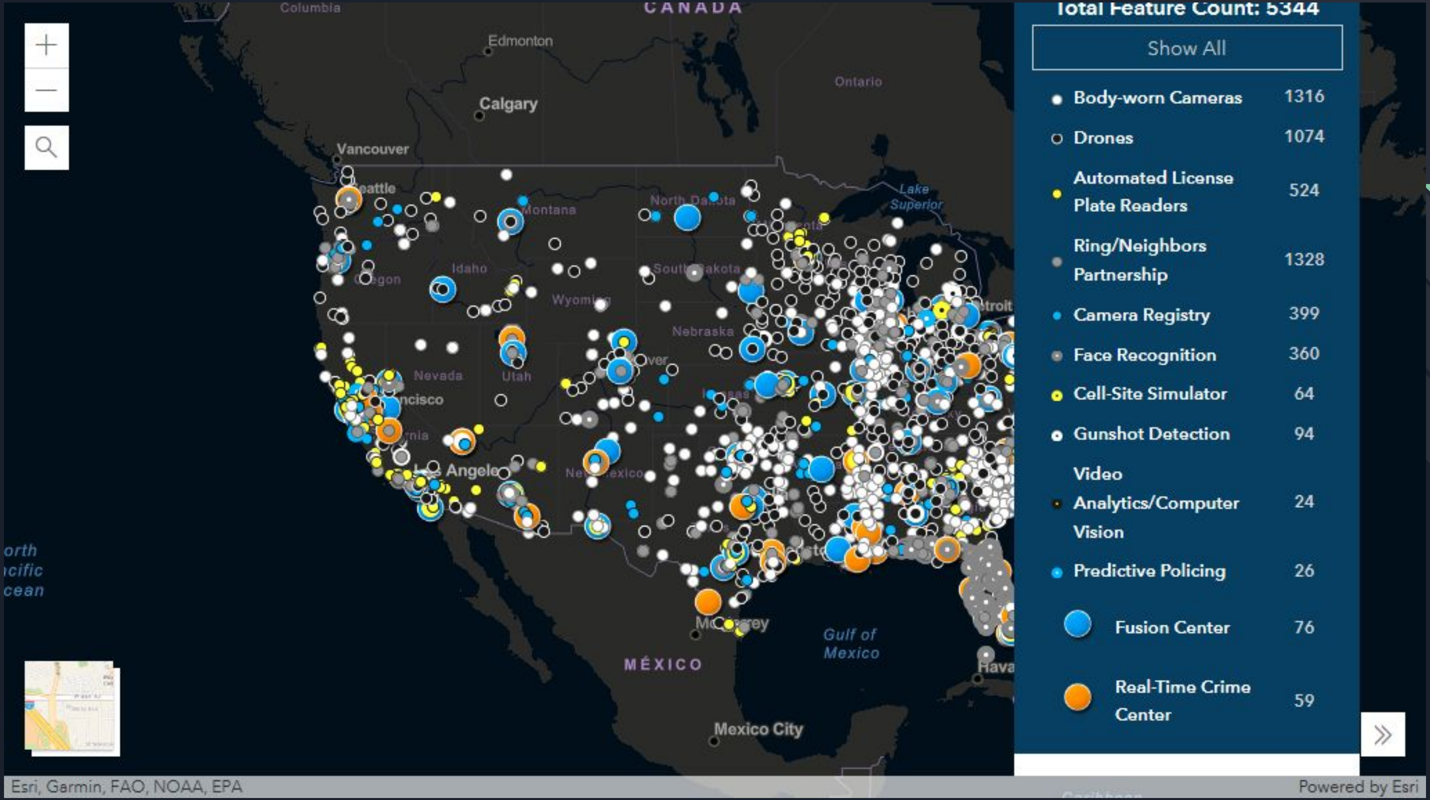
https://www.inquirer.com/news/philly-protests-arrests-fbi-lore-elisabeth-blumenthal-george-floyd-20200617.html



https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database https://www.vox.com/recode/2020/7/21/21332653/portland-oregon-protests-feds-dhs-youtube-livestream https://www.nbcnews.com/politics/justice-department/social-media-posts-help-feds-arrest-those-committing-violence-floyd-n1225081

Open Source Tools Against State Surveillance

https://atlasofsurveillance.org/



Total Feature Count: 5344

Show All

●	Body-worn Cameras	1316
○	Drones	1074
●	Automated License Plate Readers	524
●	Ring/Neighbors Partnership	1328
●	Camera Registry	399
●	Face Recognition	360
●	Cell-Site Simulator	64
●	Gunshot Detection	94
●	Video Analytics/Computer Vision	24
●	Predictive Policing	26
●	Fusion Center	76
●	Real-Time Crime Center	59

YAY WE ARE JUST BEGINNING!

- Surveillance Self-Defense by the Electronic Frontier Foundation
- "Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance" by Freedom of the Press Foundation
- Security in-a-box by Front Line Defenders and Tactical Technology Collective
- https://cpj.org/reports/2012/04/technology-security.php

FBIs guide to digital secuirty https://assets.documentcloud.org/documents/7048846/Digital-Exhaust-Opt-Out-Guide-for-LE-Partners.pdf

Some add-ons we've found to be useful:

Warning: Some of these add-ons or programs can cause your browser to operate slower or differently.

HTTPS Everywhere: https://www.eff.org/https-everywhere

Encrypts your communications with many major websites.

Privacy Badger: https://www.eff.org/privacybadger

Automatically learns to block invisible tracker.

Privacy Possum: https://addons.mozilla.org/en-US/firefox/addon/privacy-possum/

Stops commercial tracking methods by reducing and falsifying the data gathered by tracking companies.

uBlock Origin: https://www.ublock.org/

Block Ads, Pop Ups, and Trackers.

uMatrix: https://github.com/gorhill/uMatrix

Point and click matrix to filter net requests according to source, destination and type.

Disconnect: https://disconnect.me/

Tracking protection for your desktop or mobile browser.

Ghostery: Ghostery

Control over ads and tracking technologies to speed up page loads.

Shodan: https://www.shodan.io/

A search engine that lets users find specific types of computers connected to them.

Privacy.com: https://privacy.com/home

For making online purchases semi-anonymously, while also being able to set limits per-transaction.

Facebook Container: https://addons.mozilla.org/en-US/firefox/addon/facebook-container/

Automatically isolates Facebook trackers, cookies, and more.

Foxy Proxy: https://getfoxyproxy.org/

Proxy and VPN management tool as a Firefox addon.

How to: Use Tor for Android
How to: Use Tor for Linux
How to: Use WhatsApp on iOS
How to: Use WhatsApp on Android
How to: Use Signal for Android
How to: Avoid Phishing Attacks
How to: Enable Two-factor Authentication
How to: Use OTR on Linux
How to: Use Tor on macOS
How to: Delete Your Data Securely on macOS
How to: Delete Your Data Securely on Windows
How to: Delete your Data Securely on Linux
How to: Use Signal on iOS
How to: Use PGP for macOS
How to: Use PGP for Linux
How to: Use Tor for Windows
How to: Use PGP for Windows
How to: Use KeePassXC
How to: Encrypt Your Windows Device
How to: Encrypt Your iPhone
How to: Circumvent Online Censorship
How to: Use OTR for macOS

More guides for digital privacy:

Citizen Lab has this Security Planner

Probably the most relevant guide is the Bristol Anarchist Federations Guide to Online Security: An Anarchists Guide for Everyone. This is a very thorough guide on mitigating risk on many levels.

Next we have a classic. The Jolly Rogers Security Guide for Beginners. This guide is a compendium of many other guides. Almost everything you could want to know about digital security, can be found here.

Electronic Frontier Foundation: Surveillance Self Defense This is an amazing tool, probably one of the most valuable tools on this whole list. We can not recommend this enough.

Private and state-sponsored organizations are monitoring and recording your online activities, privacytools.io provides services, tools and knowledge to protect your privacy against global mass surveillance. PrivacyTools.io

Another excellent source for digital security is Freedom of the Press Foundation

And finally, this guide by Paranoid Bible:
https://pastebin.com/8zGxwtEB

Email Privacy Tools

Email Trace (https://www.ip-adress.com/trace_email/)
Have I Been Pwned (https://haveibeenpwned.com/)
Email Privacy Tester (https://emailprivacytester.com/)
Email IP Leak (http://emailipleak.com/-)
SpyCloud Early Warning Breach Detection (https://spycloud.com/)HTML5

HTML Privacy Tools

HTML5 Features Detection (https://browserleaks.com/features)
HTML5 Test (http://html5test.com/)
WebRTC Leak Test (https://www.perfect-privacy.com/en/tests/webrtc-leaktest)
WebRTC Test (https://ipleak.net/)
HTML5 Geolocation Test (https://www.browserleaks.com/geo)
Hard Drive Fill Test (http://www.filldisk.com/)
Battery Status API (https://pstadler.sh/battery.js/)
Canvas Fingerprinting (https://www.browserleaks.com/canvas)

IP Leaks

Content Filters and Proxy Test (https://www.browserleaks.com/proxy)
DNS Spoofability Test (https://www.grc.com/dns/dns.htm)
DNS Leak Test (https://www.dnsleaktest.com/)
DNSSEC Resolver Test (http://dnssec.vs.uni-due.de/)
Connection Test (https://en.internet.nl/test-connection/)
IP Magnet (http://ipmagnet.services.cbcdn.com/)
Whois Test (https://browserleaks.com/ip)
Torrent IP Check (http://checkmyip.torrentprivacy.com/)
I Know What You Download (https://iknowwhatyoudownload.com/)
SSL Heartbleed Test
(https://sslanalyzer.comodoca.com/heartbleed.html)
SSL Check (https://www.ssllabs.com/ssltest/)
How's My SSL (https://www.howsmyssl.com/)

Improved Tests

Browser Privacy Test
(https://tenta.com/test/)
Browser Spy
(http://browserspy.dk/)
Am I Unique
 (https://amiunique.org/fp)
Cross Browser Fingerprinting Test
(http://uniquemachine.org/)
Panopticlick
(https://panopticlick.eff.org/)
Jondonym Full Anonymity Test
 (http://ip-check.info/?lang=en)
Web Privacy Check
 (https://ipinfo.info/html/privacy-check.php)
Java Test
 (https://www.java.com/en/download/installed.jsp)
Flash Player System Test
 (https://browserleaks.com/flash)
Silverlight Test
 (https://browserleaks.com/silverlight)

Miscellaneous Tests

BrowserRecon
(http://www.computec.ch/projekte/browserrecon/?s=scan)
Redirect Test Page
(https://jigsaw.w3.org/HTTP/300/Overview.html)
System Fonts Detection
(https://www.browserleaks.com/fonts)
Universal Plug n'Play (UPnP) Internet Exposure Test
(https://www.grc.com/su/upnp-rejected.htm)
JavaScript Browser Information
(https://browserleaks.com/javascript)
Evercookie Test
(https://samy.pl/evercookie/)
Do Not Track
(https://www.browserleaks.com/donottrack)
Browser Referer Headers
(https://www.darklaunch.com/tools/test-referer)
Popup Blocking Tests
(http://www.kephyr.com/popupkillertest/test/test1.html)
HTTP Header Viewer
(http://www.ericgiguere.com/tools/http-header-viewer.html)
Device Info
(https://www.deviceinfo.me/)