

Cybersecurity Awareness for Humans

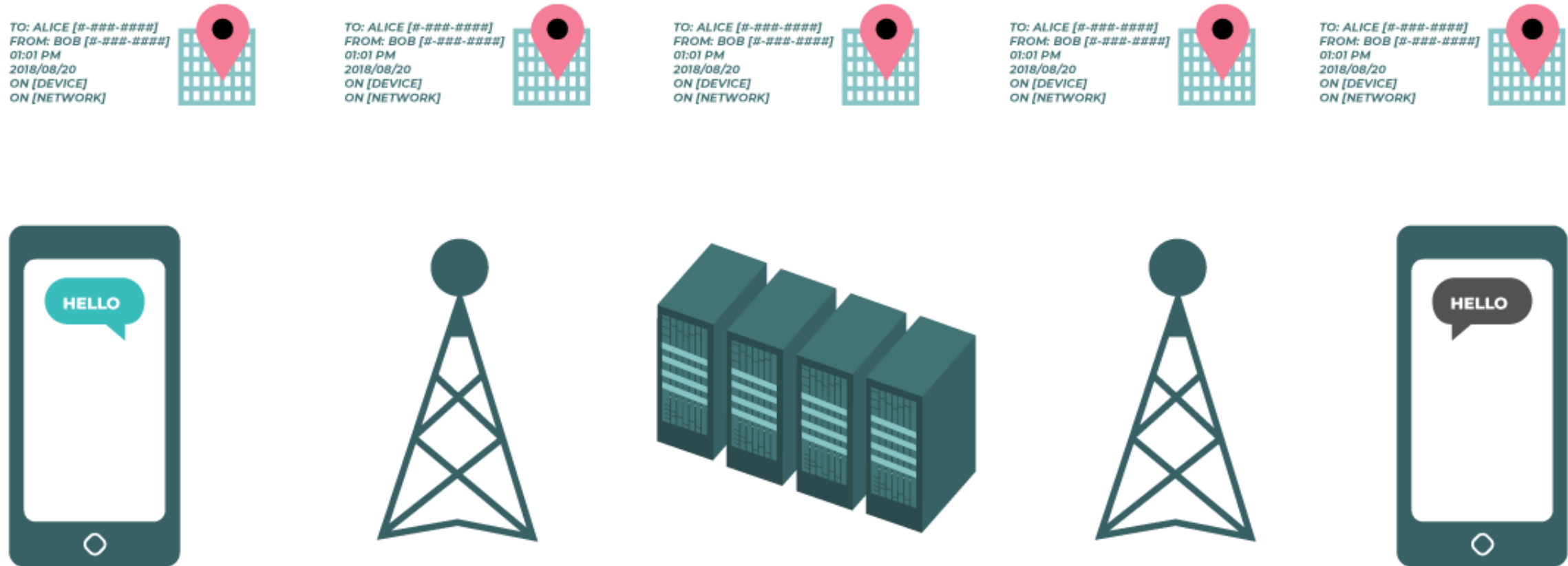
1984 is Here:

The good news is that you can control what technology you allow into your life (to an extent).

Main Topics

- What is collected and how it's used.
- Basic security practices.
- Software choices.
- Hardware choices.

Mass Surveillance of Metadata



Can collect more
than just metadata

<https://www.npr.org/sections/thetwo-way/2014/03/18/291165247/report-nsa-can-record-store-phone-conversations-of-whole-countries>

Report: NSA Can Record, Store Phone Conversations Of Whole Countries

MARCH 18, 2014 · 3:11 PM ET



Eyder Peralta



Nicolas Armer/DPA/LANDOV

Citizens in US can't be targeted, but can be caught up in sweeps of data for foreign nationals.

<https://www.eff.org/deeplinks/2024/04/us-senate-and-biden-administration-shamefully-renew-and-expand-fisa-section-702-0>

U.S. Senate and Biden Administration Shamefully Renew and Expand FISA Section 702, Ushering in a Two Year Expansion of Unconstitutional Mass Surveillance


BY [MATTHEW GUARIGLIA](#), [ANDREW CROCKER](#), [CINDY COHN](#), AND [BRENDAN GILLIGAN](#) | APRIL 22, 2024



Warrantless Purchase of Commercial Web Browsing Data

The National Security Agency has been buying Americans' web browsing data from commercial data brokers without warrants, intelligence officials disclosed in documents made public by a US senator Thursday.

<https://www.cnn.com/2024/01/26/tech/the-nsa-buys-americans-internet-data-newly-released-documents-show>



Trump Taps Palantir to Compile Data on Americans

Creating detailed portraits of Americans based on government data is not just a pipe dream. The Trump administration [has already sought access](https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html) to hundreds of data points on citizens and others through government databases, including their bank account numbers, the amount of their student debt, their medical claims and any disability status.

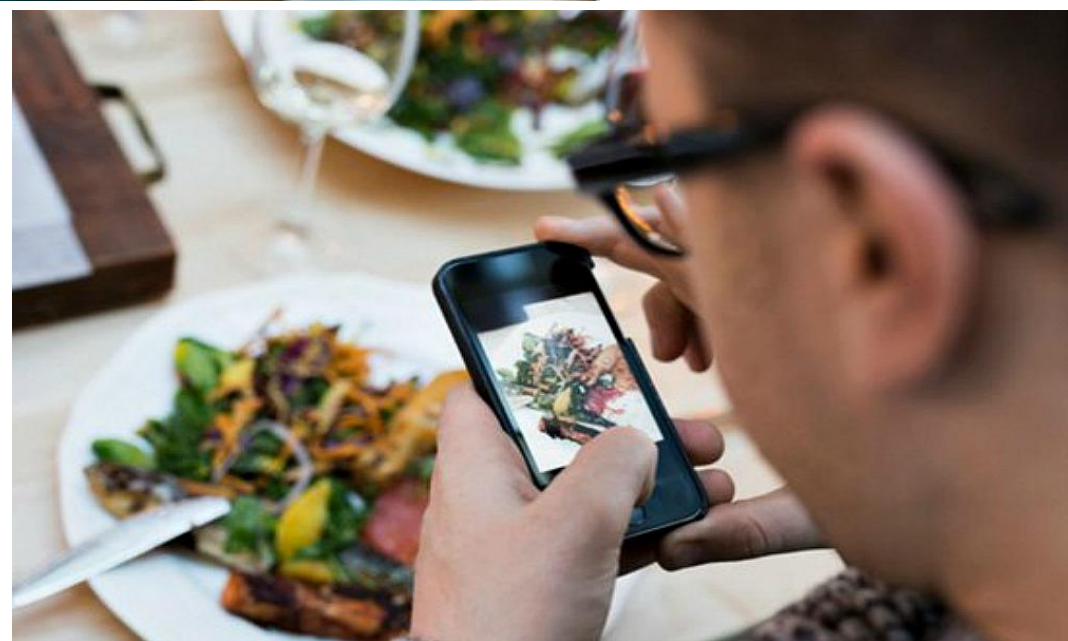
- <https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html>

Re-Identification of Anonymized Data

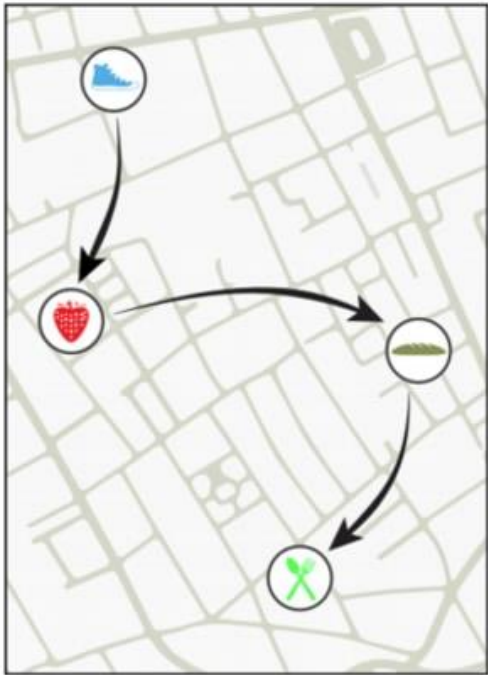
Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization

Paul Ohm, UCLA Law Review, Vol. 57, p. 1701, 2010.

Computer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name for techniques for protecting the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated they can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease.



Anonymized Credit Card Statement



shop	user_id	time	price	price_bin
	7abc1a23	09/23	\$97.30	\$49 – \$146
	7abc1a23	09/23	\$15.13	\$5 – \$16
	3092fc10	09/23	\$43.78	\$16 – \$49
	7abc1a23	09/23	\$4.33	\$2 – \$5
	4c7af72a	09/23	\$12.29	\$5 – \$16
	89c0829c	09/24	\$3.66	\$2 – \$5
	7abc1a23	09/24	\$35.81	\$16 – \$49

Phone Metadata

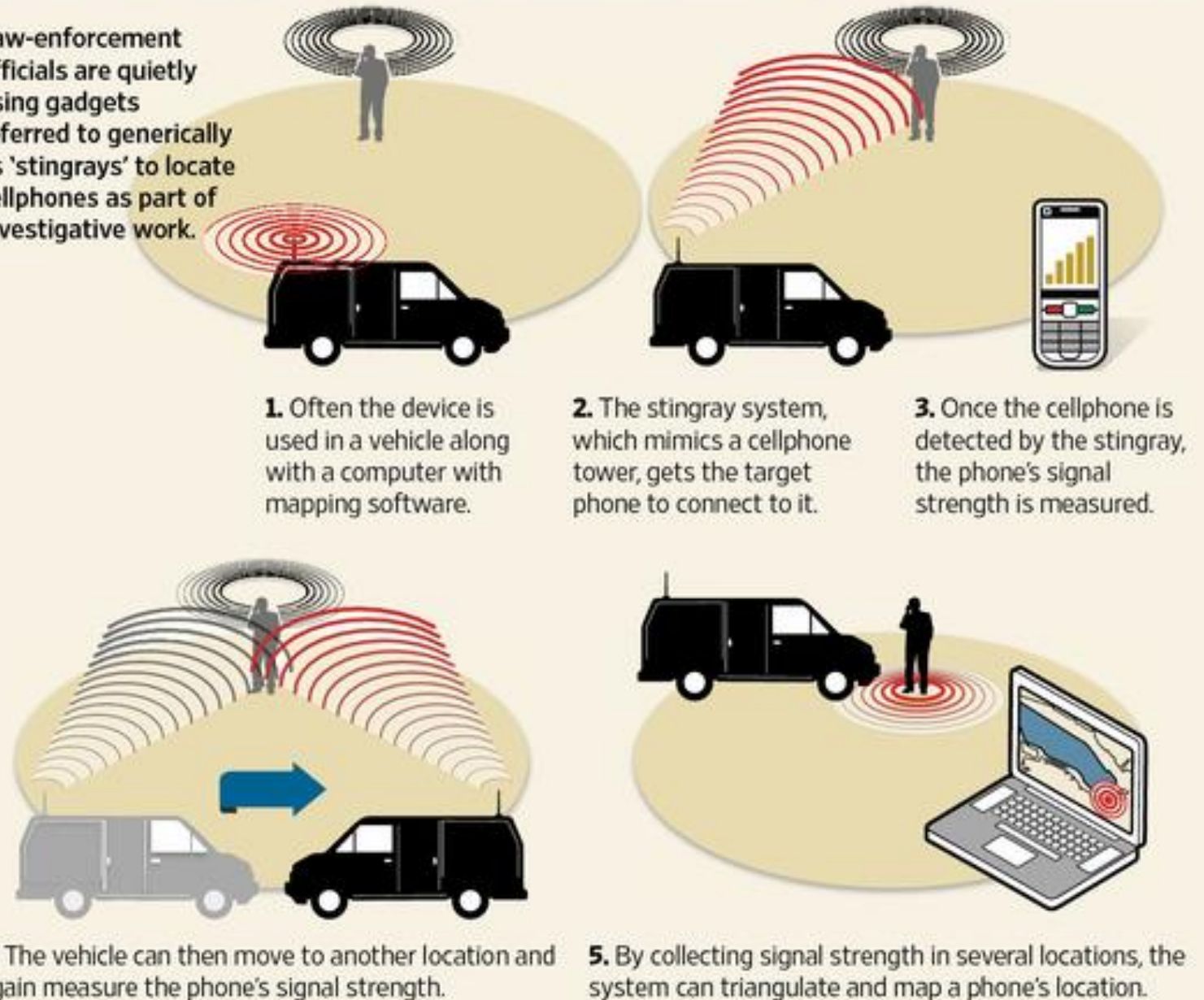
A1 : X ✓ fx ID													
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	ID	FULL_NAME	FIRST_NAME	LAST_NAME	CALLING_NBR	CALLED_NBR	START_DATE	END_DATE	DURATION	CITY	STATE	ADDRESS	CELL_SITE
2	1	RalphJordan	Ralph	Jordan	8-(921)364-8515	3-(230)472-4011	1419197491	1419198397	906	Fair Oaks	CA	27834 Glend	80
3	2	PamelaPowell	Pamela	Powell	2-(270)359-8113	2-(833)444-8281	1416290807	1416292942	2135	West Sacram	CA	35593 Portag	51
4	3	AnnaGibson	Anna	Gibson	3-(307)801-5521	9-(490)378-2330	1417817803	1417820157	2354	Sacramento	CA	1323 El Cami	102
5	4	BeverlyKelly	Beverly	Kelly	7-(423)821-7199	3-(307)801-5521	1417220166	1417223469	3303	Folsom	CA	28473 Hanzo	81
6	5	RobertBowman	Robert	Bowman	7-(445)366-2890	2-(833)444-8281	1415288003	1415289004	1001	Sacramento	CA	4 Waubesa P	32
7	6	WalterWright	Walter	Wright	9-(375)425-6362	8-(618)141-5320	1414689052	1414691454	2402	Orangevale	CA	97 Briar Cres	79
8	7	WalterWright	Walter	Wright	9-(375)425-6362	3-(812)536-3510	1419461129	1419462362	1233	Sacramento	CA	11746 Moose	59
9	8	AnnaGibson	Anna	Gibson	3-(307)801-5521	5-(606)804-8887	1418418016	1418421169	3153	Sacramento	CA	088 Spohn Di	67
10	9	ArthurWest	Arthur	West	8-(396)221-0695	5-(923)984-7542	1415671824	1415673017	1193	Sacramento	CA	4 Declaratio	45
11	10	EricMccoy	Eric	Mccoy	4-(195)345-0796	2-(018)291-3145	1414817602	1414822092	4490	Sacramento	CA	2 Badeau Poi	19
12	11	FredCarpenter	Fred	Carpenter	0-(512)960-7007	4-(360)048-0339	1415207223	1415208636	1413	Clarksburg	CA	920 Thompsc	49
13	12	IreneWood	Irene	Wood	4-(854)454-5378	5-(461)543-0594	1417390459	1417391574	1115	Antelope	CA	3 Union Lane	7
14	13	AmandaJordan	Amanda	Jordan	0-(169)877-8366	4-(864)125-8623	1415196725	1415197499	774	Sacramento	CA	39666 Spalg	29
15	14	AlanLittle	Alan	Little	0-(887)175-3438	6-(069)658-1639	1417331895	1417336818	4923	Sacramento	CA	14 Golf View	100
16	15	AdamLynch	Adam	Lynch	3-(946)780-1280	8-(618)141-5320	1417303280	1417307598	4318	Sacramento	CA	367 Kenwoo	60
17	16	KathyWard	Kathy	Ward	4-(924)540-2989	8-(170)153-7171	1414230633	1414234846	4213	Sacramento	CA	612 Clove Tr	39
18	17	ElizabethRamirez	Elizabeth	Ramirez	7-(138)030-2131	8-(618)141-5320	1418520935	1418521317	382	Sacramento	CA	9055 Meadow	68
19	18	AlanFields	Alan	Fields	3-(436)534-0022	0-(169)877-8366	1414528885	1414530483	1598	Citrus Heighl	CA	524 Manufac	83
20	19	PamelaPowell	Pamela	Powell	2-(270)359-8113	3-(631)865-3020	1415652313	1415652568	255	Sacramento	CA	24 Arapahoe	9
21	20	AmandaJordan	Amanda	Jordan	0-(169)877-8366	9-(768)433-4919	1415664451	1415667634	3183	North Highla	CA	47400 Dayton	37
22	21	RobinGonzalez	Robin	Gonzalez	2-(018)291-3145	6-(045)502-0137	1419088494	1419090809	2315	Sacramento	CA	056 Del Mar	42
23	22	HeatherFox	Heather	Fox	2-(413)834-5844	8-(618)141-5320	1417966877	1417971563	4686	Carmichael	CA	40161 Cardin	98
24	23	HeatherFox	Heather	Fox	2-(413)834-5844	8-(618)141-5320	1417966877	1417971563	4686	Carmichael	CA	40161 Cardin	98

Stingray Surveillance

Reports of its use at protests since 2003:
<https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers>

How a 'Stingray' Cellphone-Tracking Device Works

Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.



Source: WSJ research and government documents



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.

Take Home: The information you reveal can be used against you in unexpected ways.

Mass Surveillance: Palestine

- **Did Israel know over 80 percent of those it killed in Gaza were civilians?**
- *A leaked military report suggests only 17 percent of those killed in Gaza were fighters.*
- <https://www.aljazeera.com/news/2025/8/24/did-israel-know-over-80-percent-of-those-it-killed-in-gaza-were-civilians>

Questions and Answers: Israeli Military's Use of Digital Tools in Gaza

One is based on mobile phone tracking to monitor the evacuation of Palestinians from parts of northern Gaza. Another, which the military calls “The Gospel,” generates lists of buildings or other structural targets to be attacked. Another, which the military calls “Lavender” assigns ratings to people in Gaza related to their suspected affiliation with Palestinian armed groups for purposes of labeling them as military targets. “Where’s Daddy?” purports to determine when a target is in a particular location so they can be attacked there.

<https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza>

What can I do?

- Recognize that no electronic device is surveillance proof.
- Be prepared to take a number of steps to secure your digital footprint.
- Even if you are not a target, if you are security-conscious that will help other people.

No steps are 100% surveillance proof

If you don't want to be monitored,
don't communicate electronically (or
near electronic devices).

Cybersecurity Steps: Password

- **Long**—at least 16 characters long (even longer is better).
- **Random**—like a string of mixed-case letters, numbers and symbols (the strongest!) or a passphrase of 4 –7 random words.
- **Unique**—used for one and only one account.
- Long passwords with word: 4-5 words strung together for at least 25 characters: *GreenLemurSandTravelMagic*.

Password Manager

- Provide a high level of password security, but you have to keep your login for your password manager secure.
- Have to trust the password manager is reliable (and stays that way).

Password Managers that appear to be good:

Proton Pass: <https://www.proton.me/pass>


1Password: <https://www.1password.com>

Dashlane: <https://www.dashlane.com>

Don't Use Biometrics

- Facial recognition
- Iris scan
- Voiceprint
- Fingerprint

Gives personal data to company.
Easiest to steal.




The illustration features a blue padlock in the center. Above the padlock is a circular graphic containing a fingerprint, and below it is a circular graphic containing an eye. Both circular graphics have a grid pattern and corner brackets, suggesting a scanning or framing process. The entire graphic is set against a light blue background.

Biometrics

[,bī-ō-'me-triks]

Digital security methods that rely on biological or physiological attributes to prevent data breaches.

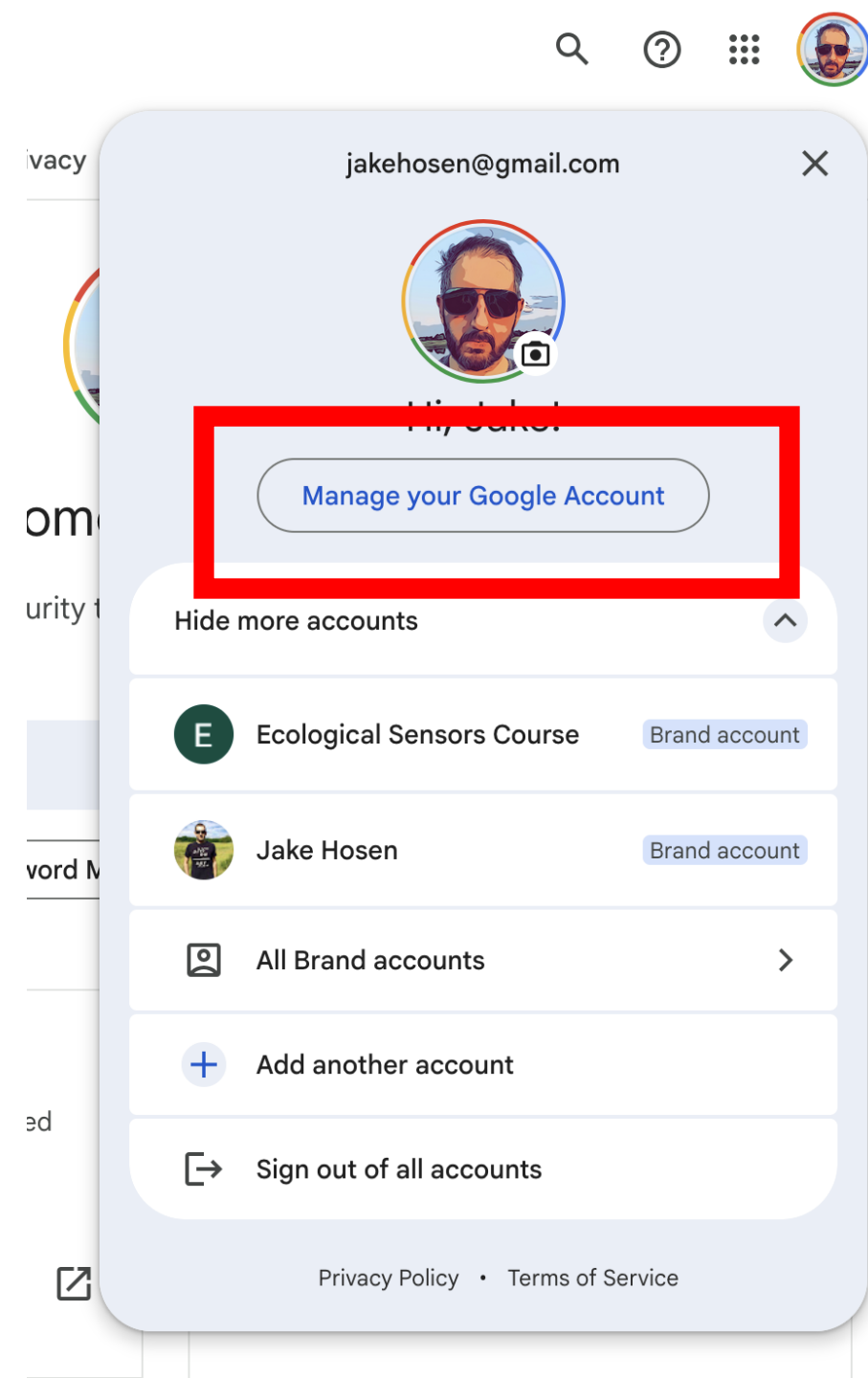
 Investopedia

2 Factor Authentication (2FA)

- **It's annoying, but you should turn it on wherever possible.**
- **Apps for 2 Factor Authentication:**
 - 2FAS: 2fas.com
 - Aegis: getaegis.app (Android Only)
 - Duo Mobile
 - Microsoft Authenticator
 - Google Authenticator

Turn on Google 2 Factor

- While logged in on any google page, click your user icon.
- Select “Manage your Google Account”





Personal info

Data & privacy

Security

People & sharing

Payments & subscriptions

Settings and recommendations to help you keep your account secure

You have security tips

Security tips found in the Security Checkup



[Review security tips](#)

Recent security activity

No security activity or alerts in the last 28 days

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date



2-Step Verification

2-Step Verification is off



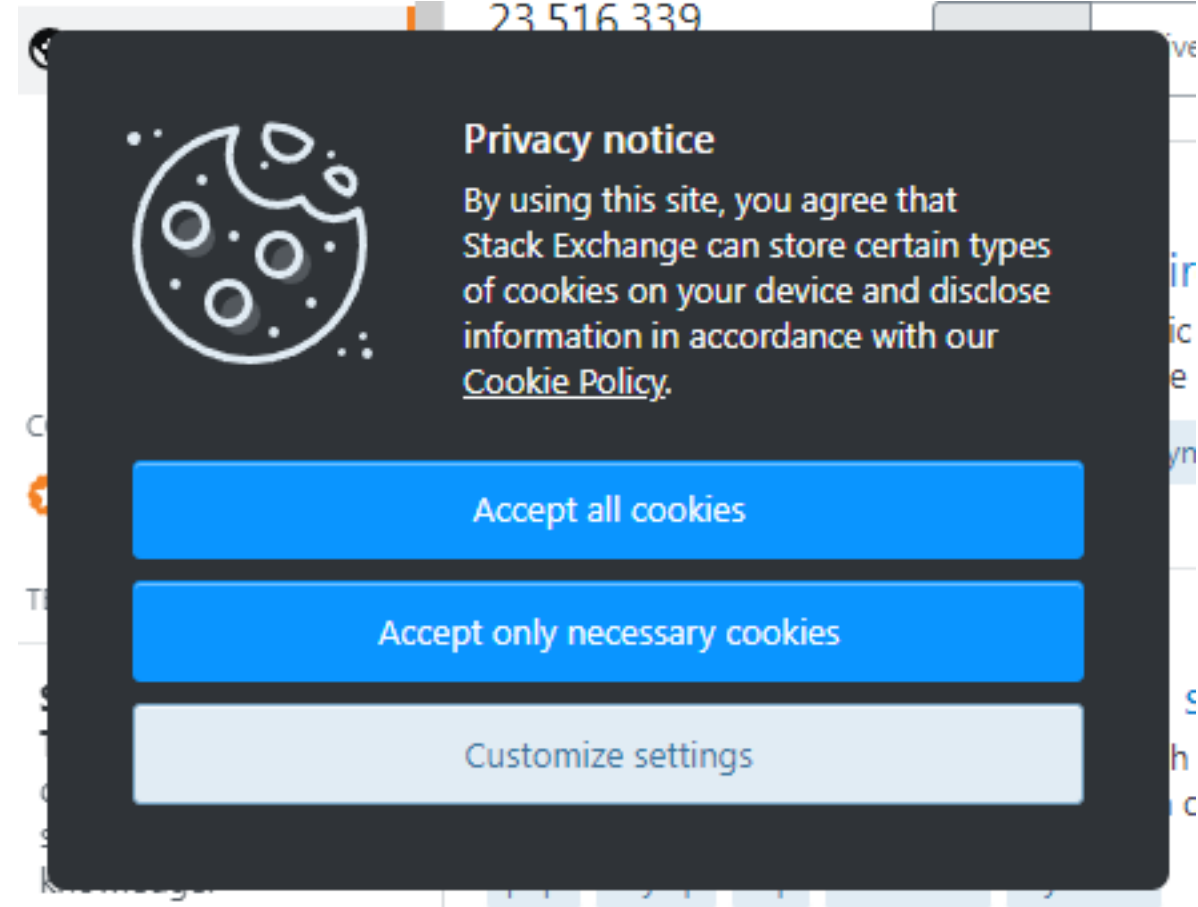
Software: General Rules

- Keep your software up to date, particularly your device operating system (Windows, MacOS, Android, IOS, etc.)
- Use open-source software when possible.
- Installing software through an App Store will decrease the likelihood of installing malicious software.



Cookies

- Tokens that your browser saves with information for each website.
- Helps keep you logged into services. This is good if you are using a secure computer because you have to enter your password less.
- Downside is that cookies can sometimes collect too much information.
- **Recommendation:** Keep them on but block unnecessary cookies whenever possible.



Browser Security Settings

- **Turn Off** *Third Party Cookies*.
- **Turn On** *Request Websites Do Not Track*.
- **Turn On** *Show complete website address*.
- **Turn On** *require https*.
- **Turn Off** *Location Services*.
- Browser check-up tool:
<https://coveryourtracks.eff.org/>

Brave Browser

Firefox

SettingsHistoryBookmarksDownloadsWalletRewards

Get started

Appearance

Content

Shields

Privacy and security

Web3

Leo

Sync

Search engine

Extensions

Autofill and passwords

Languages

Downloads

Accessibility

System

Shields

Block trackers and ads which follow you across the web.

These are the default Shields settings. They apply to all websites unless you change something in the Shields panel on a particular site. Changing these won't affect your existing per-site settings.

This will block most ads on websites.

Show the number of blocked items on the Shields icon

Trackers & ads blockingStandard

Upgrade connections to HTTPSStandard

Block scripts

Block fingerprinting

Block cookiesBlock third-party cookies

Forget me when I close this site

Store contact information for future broken site reports

Content filtering

General

Home

Search

Privacy & Security

Sync

Firefox Labs

More from Mozilla

Extensions & Themes

Firefox Support

Find in Settings

Browser Privacy

Enhanced Tracking Protection



Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.

[Learn more](#)

Manage Exceptions...

☒ Standard

Balanced for protection and performance. Pages will load normally.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

Includes Total Cookie Protection, our most powerful privacy feature ever

Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. [Learn more](#)

☐ Strict

Stronger protection, but may cause some sites or content to break.

☐ Custom

Choose which trackers and scripts to block.

Website Privacy Preferences

☐ Tell websites not to sell or share my data [Learn more](#)

VPN: Encrypt your web traffic

Without VPN



User



Connection is not encrypted



Internet

With VPN



User



VPN Server



New IP



Connection encrypted



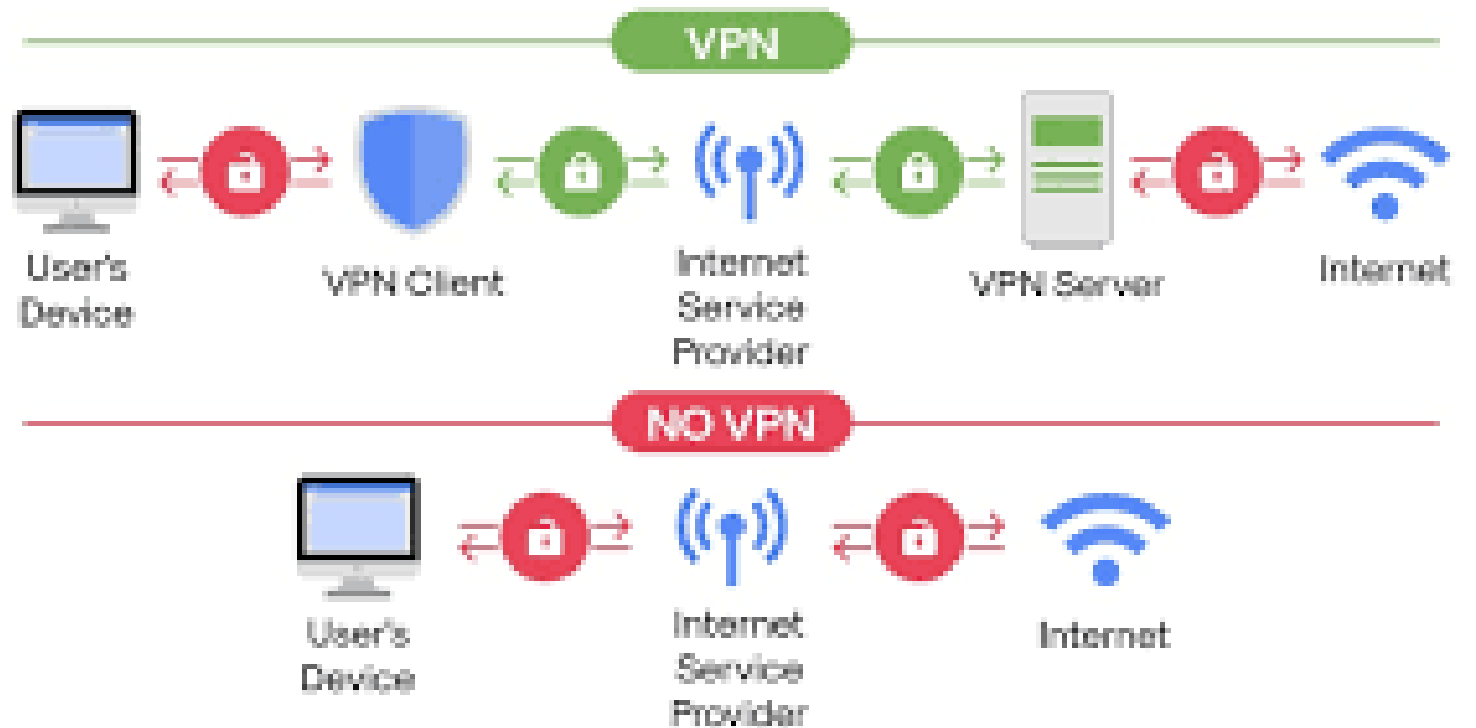
Internet

VPN Services

- Proton VPN: protonvpn.com
- Express VPN: expressvpn.com
- Nord VPN: nordvpn.com



How Does Logging Process Work



Email Security Reality

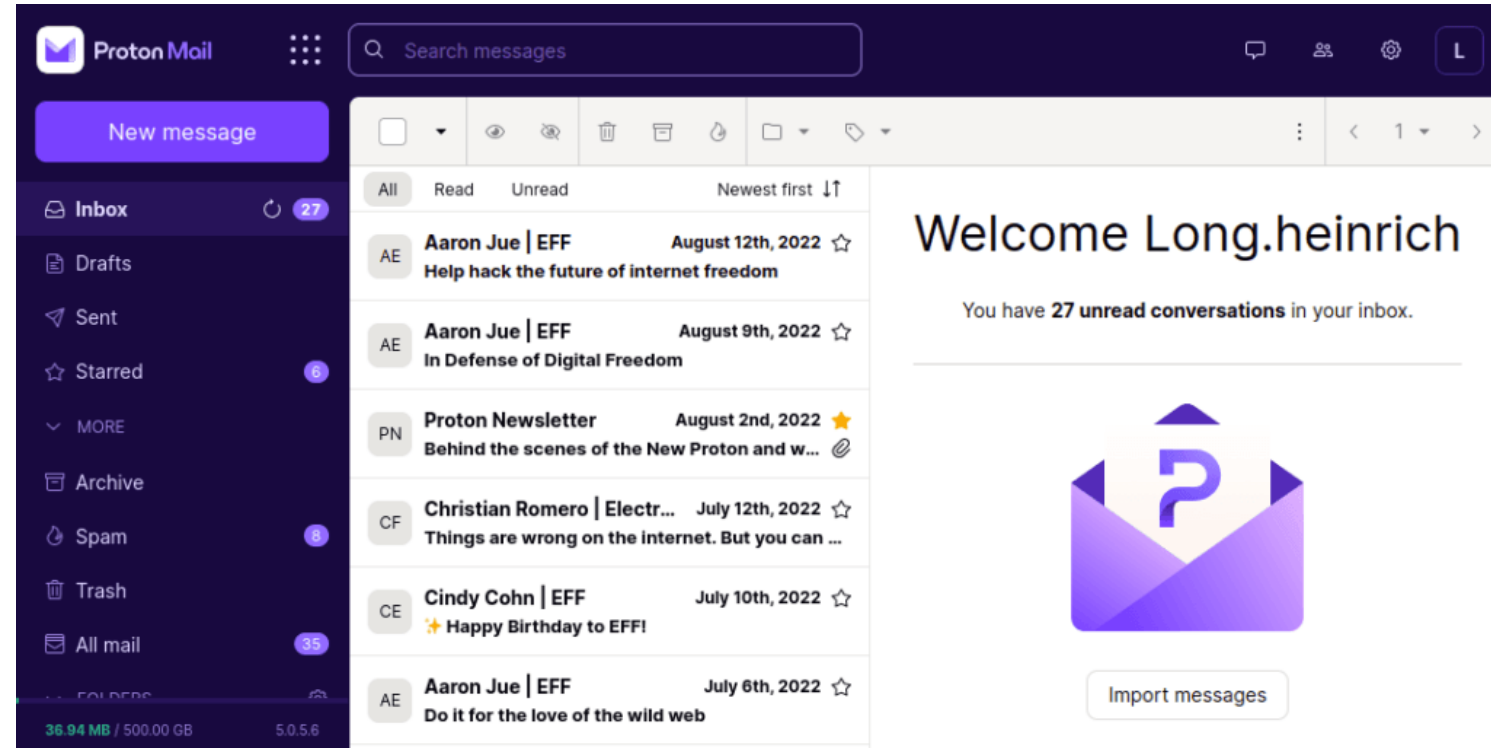
- Your boss can read your email.
- Standard email traffic is essentially unencrypted, very easy to access.
- Your email provider is very likely to hand over your data to the government without an argument.

Email Security Countermeasures

- Don't send things you don't want other people knowing via email.
- Use a secure email provider such as *Proton Mail* (proton.me). **Offers only partial protection.**
- Encrypt your email with Pretty Good Protection (PGP). **It's pretty good.**

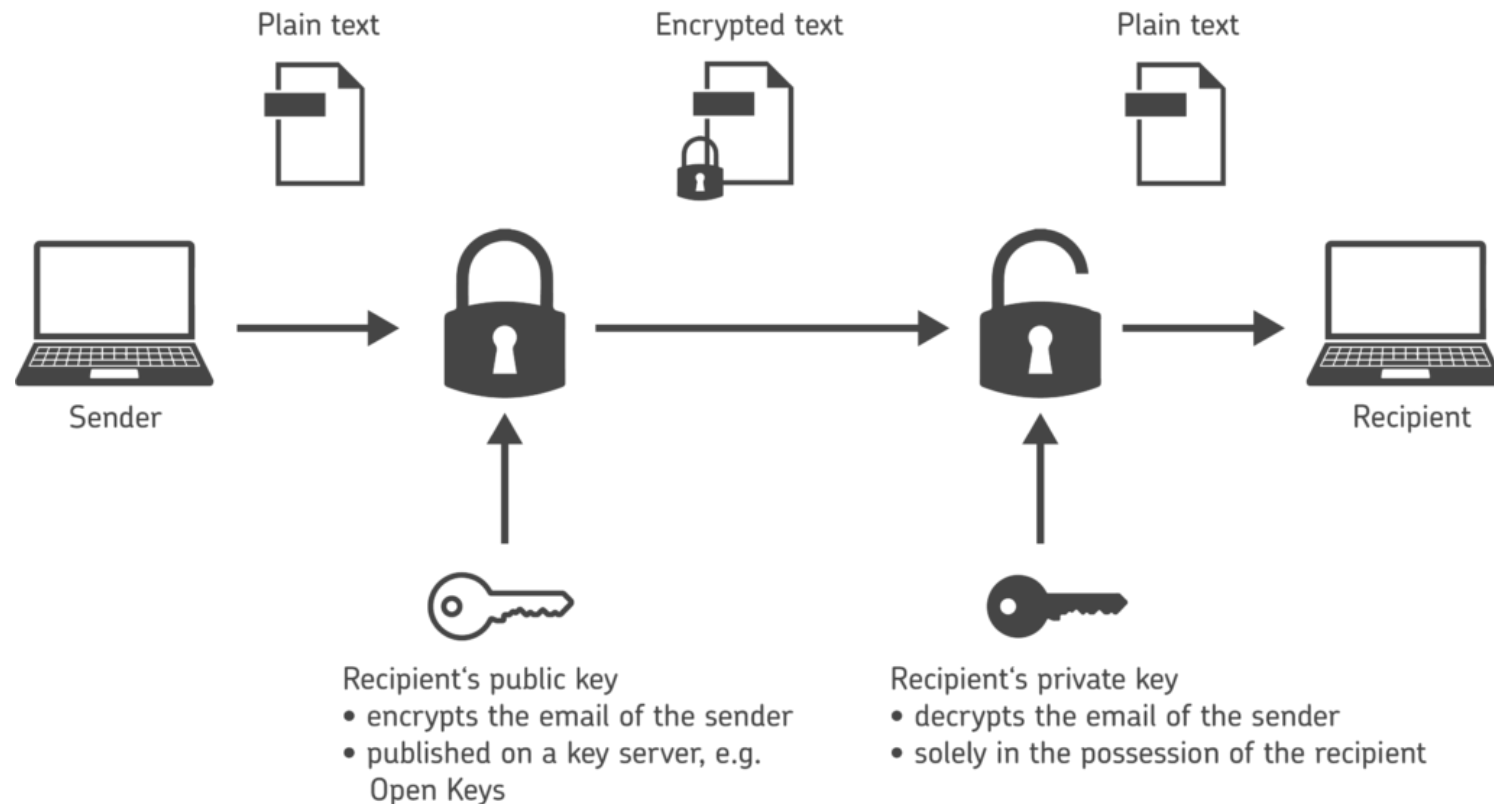
Secure email providers

- Better security between you and your provider's servers. Once the email is out in the world, protection is gone.
- Less likely to hand over your data to a government or sell your data to a third party. **We know Google and Microsoft will do this.**



Pretty Good Protection (PGP) Encryption

- GPG Suite (macos): <https://gpgtools.org/>
- GPG4WIN (Windows): <https://www.gpg4win.org/>



Fight Spam

- Check the actual email address of the sender.
- Don't click links or open attachments in any suspicious email even if their address checks out.
- Report junk/spam/phishing messages.

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

24 AM

1. Fake sender domain.
(not service@paypal-australia.com.au)



How to restore your PayPal account

2. Suspicious Subject and content.

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

3. Bad grammar

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

Click to follow link

[Log in your account now](#)

4. Hovering over link reveals suspicious URL.

PayPal Email ID PP32260008777636

10 MOST COMMON SIGNS OF A PHISHING EMAIL

Phishing continues to be the #1 attack vector for threat actors – these are the tell-tale signs you need to know.



1

AN UNFAMILIAR TONE OR GREETING

Look for language that isn't quite right – for example, a colleague or family member is a little more formal or casual than normal.



2

GRAMMAR AND SPELLING ERRORS

One of the more common signs of a phishing email is bad spelling and the incorrect use of grammar.



3

INCONSISTENCIES IN EMAIL ADDRESSES, LINKS & DOMAIN NAMES

Look for discrepancies in email addresses, links and domain names. If a link is embedded in the email, hover over the link to verify that what 'pops up' is a legitimate URL.



4

THREATS OR A SENSE OF URGENCY

Emails that threaten negative consequences or use a sense of urgency to encourage, or even demand, immediate action should always be treated with suspicion.



5

SUSPICIOUS ATTACHMENTS

If an email with an attached file is received from an unknown sender or if the recipient did not request or expect to receive the file, the email and attachment should be virus-scanned before opening.



6

UNUSUAL REQUEST

If an email is received asking for something to be done that is not the norm, it is a red flag for a potentially malicious email.



7

SHORT AND SWEET

While many phishing emails will be stuffed with details designed to offer a false sense of security, some phishing messages will have sparse information hoping to trade on their ambiguity.



8

RECIPIENT DID NOT INITIATE THE CONVERSATION

Because phishing emails are unsolicited, an often-used hook is to inform the recipient they won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment.



9

REQUEST FOR CREDENTIALS, PAYMENT INFO OR OTHER PERSONAL DETAILS

One of the most sophisticated types of phishing emails contains a link to a fake landing page the attacker created that recipients are directed to in an official-looking email. Recipients should visit the website by typing in the URL, rather than clicking on a link.



10

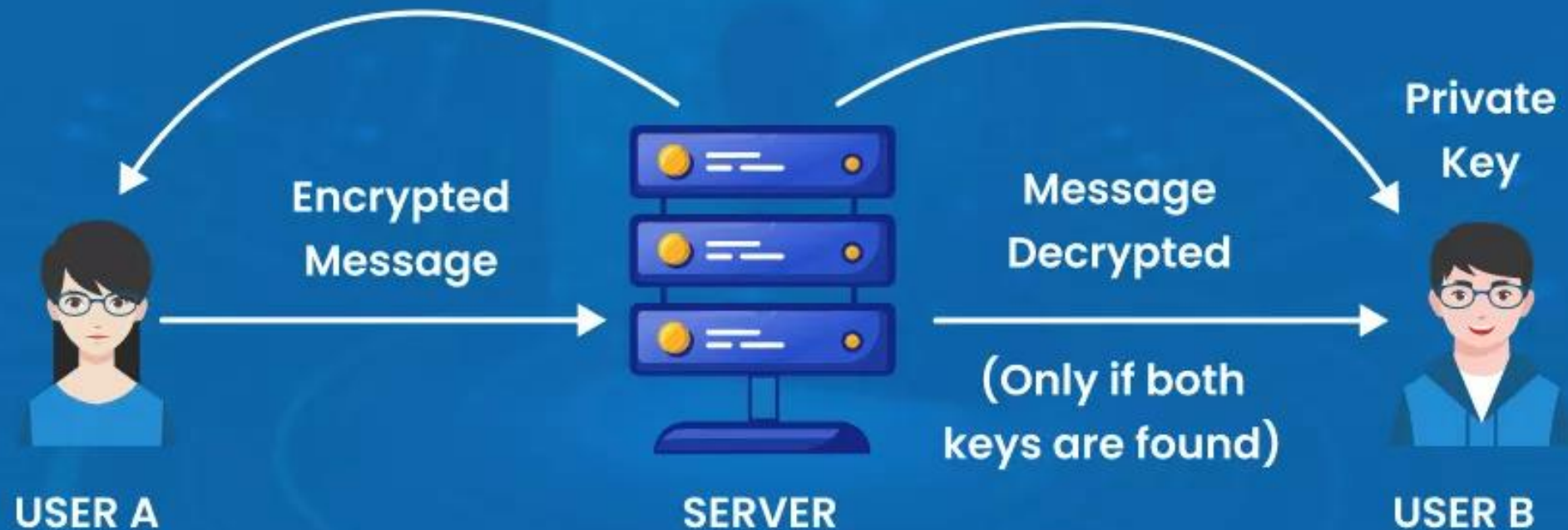
SEE SOMETHING, SAY SOMETHING

Identification is the first step in the battle against phishing. Organizations need to promote security awareness and condition employees to report potentially malicious emails.

Messaging Security

- “Basic” chats have lower security (e.g., SMS, MMS, and more recently RCS).
- Other messaging programs (e.g., Signal, Whatsapp, iMessages) now offer end to end encryption (E2EE). What is this and are they all the same?





**What is End to End Encryption (E2EE) &
How does it Work?**

Secure Messaging Services

- Closed source solutions like *Whatsapp* require you to trust that the company is managing keys properly.
- Open source options like Signal (signal.org) are more trustworthy.

Downside of Signal and other Secure Messaging Clients

- If you lose your keys you lose your data.
- True end to end encryption.
- If you lose your device and didn't back up your keys somewhere, your data are gone!

Security is Limited, Particularly for Mobile Devices

Both IOS and Android phones can be hacked without any actions on your part.

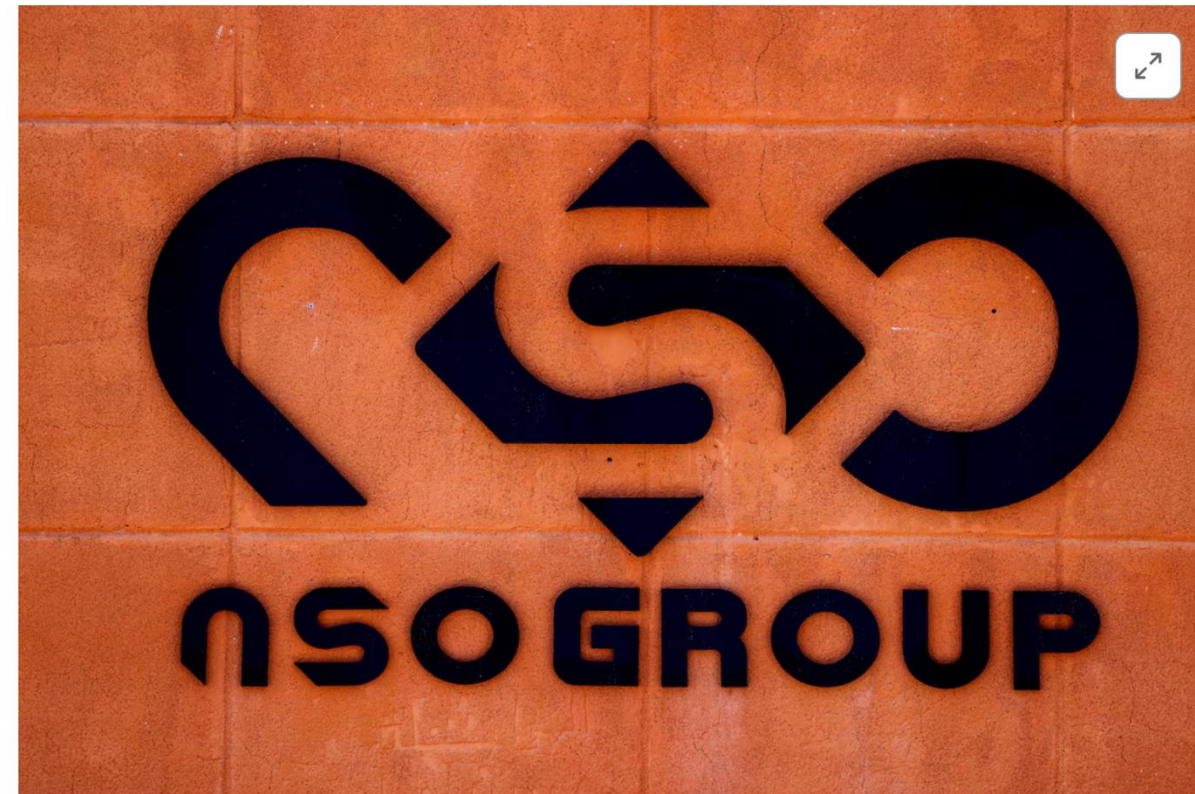
You will likely not be able to tell this has happened.

<https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/>

U.S. State Department phones hacked with Israeli company spyware - sources

By Christopher Bing and Joseph Menn

December 3, 2021 11:18 PM EST · Updated December 3, 2021



[1/2] The logo of Israeli cyber firm NSO Group at one of its branches in the Arava Desert, southern Israel July 22, 2021. REUTERS/Amir Cohen [Purchase Licensing Rights](#)



Next Step Up: Hardware

- Purchase a new phone for maximum security (less of a concern for computers).
- Do not plug your phone into USB outlets in public. Use a charging brick



Make sure you are buying secure networked devices.

- Do I need this networked device?
- Device software is often bad. Make sure device has been evaluated by known reviewers.
- Make sure you have changed all the access and management passwords.



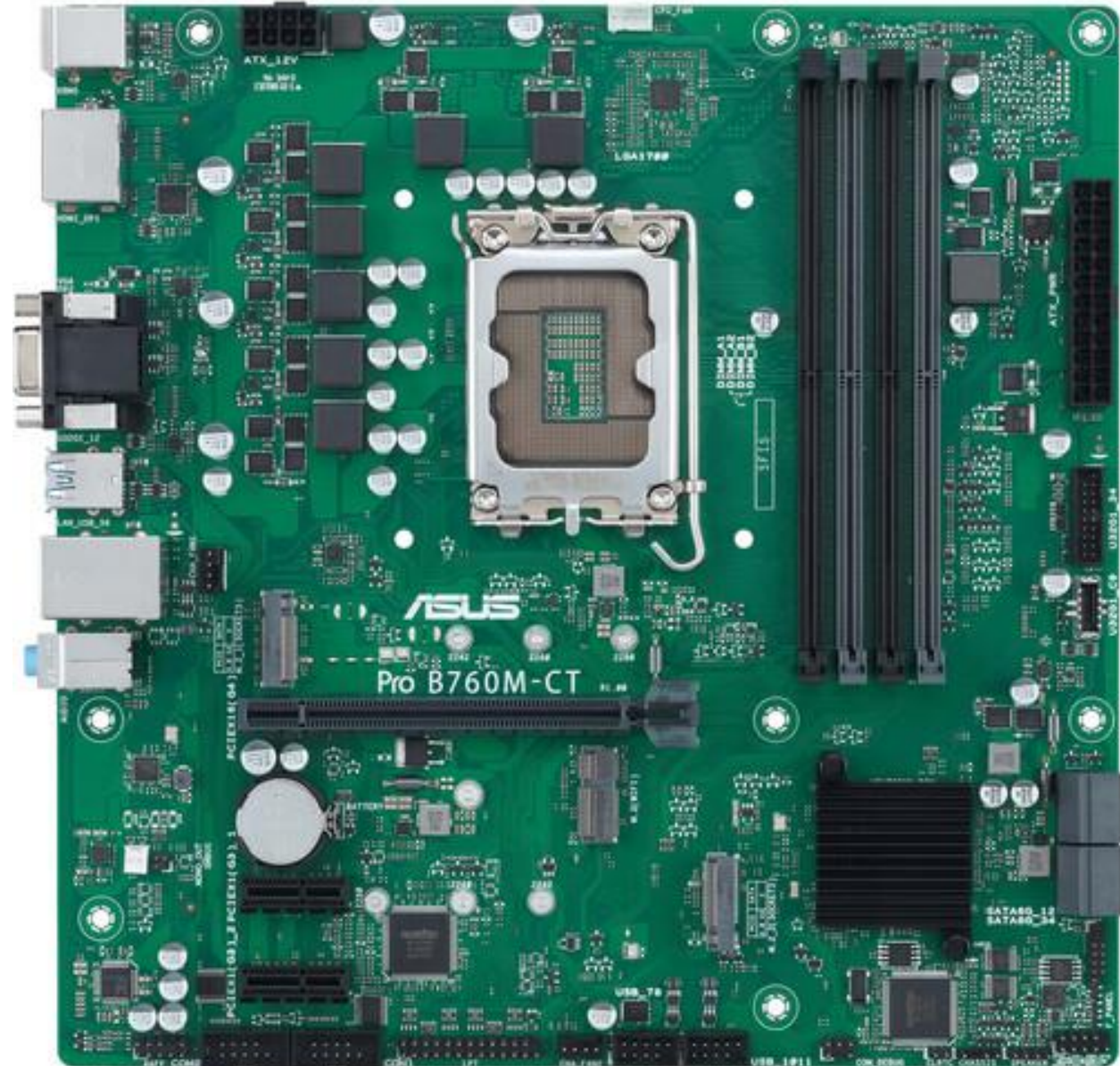
Network Security Cameras

- Your data provider may (will probably) give your data to law enforcement without a warrant.
- June 2025: 40,000 web cams on internet are accessible to public.
- Millions of devices are vulnerable (bad software, weak passwords).



Hardware Vulnerabilities

- Numerous governments want to/have installed spyware in low-level processors. This sort of surveillance is very hard to spot.
 - *Extreme Example: Hezbollah Cell Phone Attack*
- Particularly bad for internet “devices”.
- Open source software for all chips can essentially eliminate this problem, but that is very hard.



A Secure Phone

Librem 5 by Purism

(<https://puri.sm/products/librem-5/>)

This is pretty much the only option.

Downsides:

Limited networks

relatively poor battery life

uses alternative OS with fewer apps.



Laptop Available

Purism device

Limited battery.

Runs on Linux and
can require lots of
manual
configuration.

The Road Warrior



The first 14" laptop designed to protect your digital life

Ultra-portable workstation laptop that was designed chip-by-chip, line-by-line, to respect your rights to privacy, security, and freedom.

Framework

- Not quite as secure as Purism devices but much easier to use.
- Highly upgradeable.
- Still requires a power user to properly use security features.



Constant Vigilance

Just because a service, program, device is secure now does not mean that it can't be bought out by another company that will ruin it.

Thank you

Presentation: <https://jakehosen.github.io/cybersecurity-awareness.pdf>

Contact: jakehosen@proton.me

Resources

Electronic Frontier Foundation: <https://www.eff.org>

Self-Guided Cybersecurity Course:
<https://github.com/brootware/awesome-cyber-security-university>