Digital Security Training

20 minutes - Link

Protect yourself

- FOR: your livelihood, employment, admission, legal status, immigration status, etc.
- FROM: State and state collaborators Police, Feds, Canary Mission, Data Brokers, Doxing Websites, Holistic Digital Discrimination

https://remover.visiblelabs.org (open source Incongni)

Request to remove data from data brokers

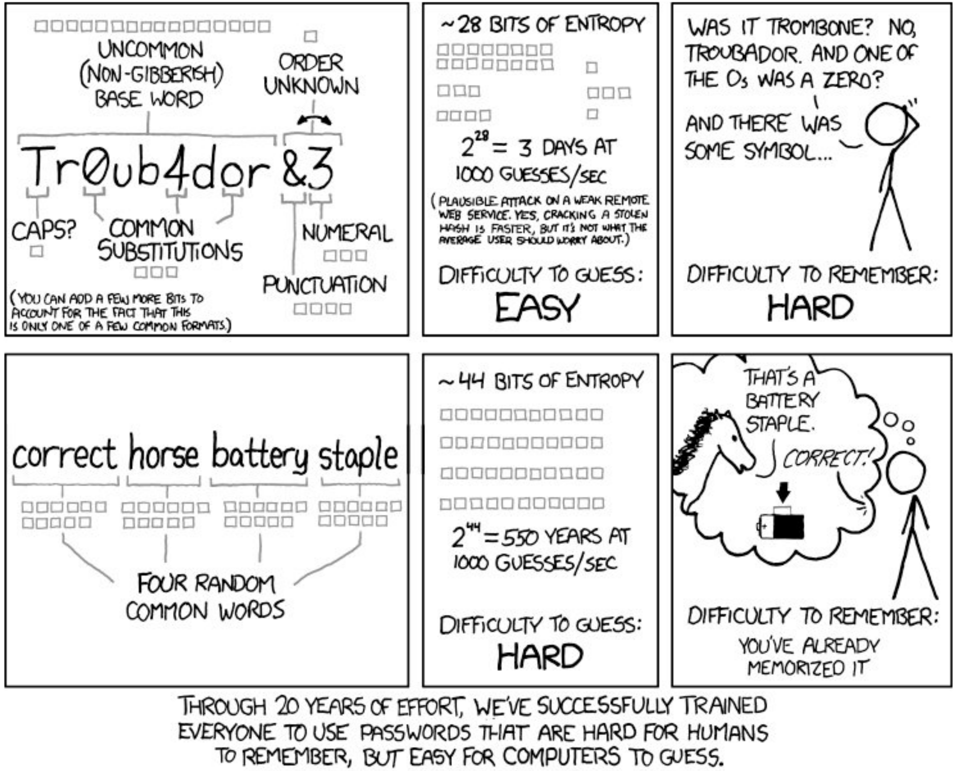
What Exactly are We Protecting?

- **PII: Personal Identifiable Information**

  Name
  Address
  Face
  Audiovisual
  SSN
  IP Address
  Credit Card
  ID #
  Any Account #
  Location
  Intrests
  Etc.

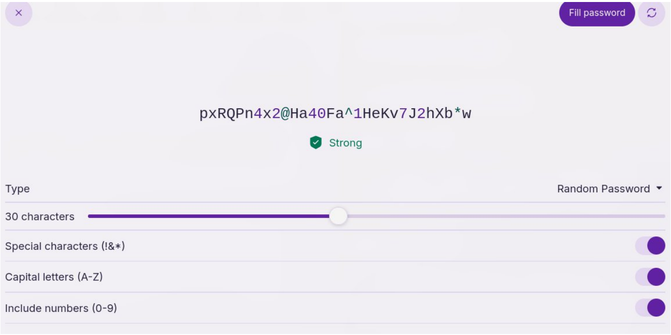
- **Doxing: Having *any* PII leaked *nonconsensually***

Use Good Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

For Master Passwords:
Follow the Correct House Battery Staple paradigm

For Everything Else:
Generate a random password using a password manager like proton pass or bitwarden



pxRQPn4x2@Ha40Fa^1HeKv7J2hXb*w

Strong

Type: Random Password

30 characters

Special characters (!&*) ●

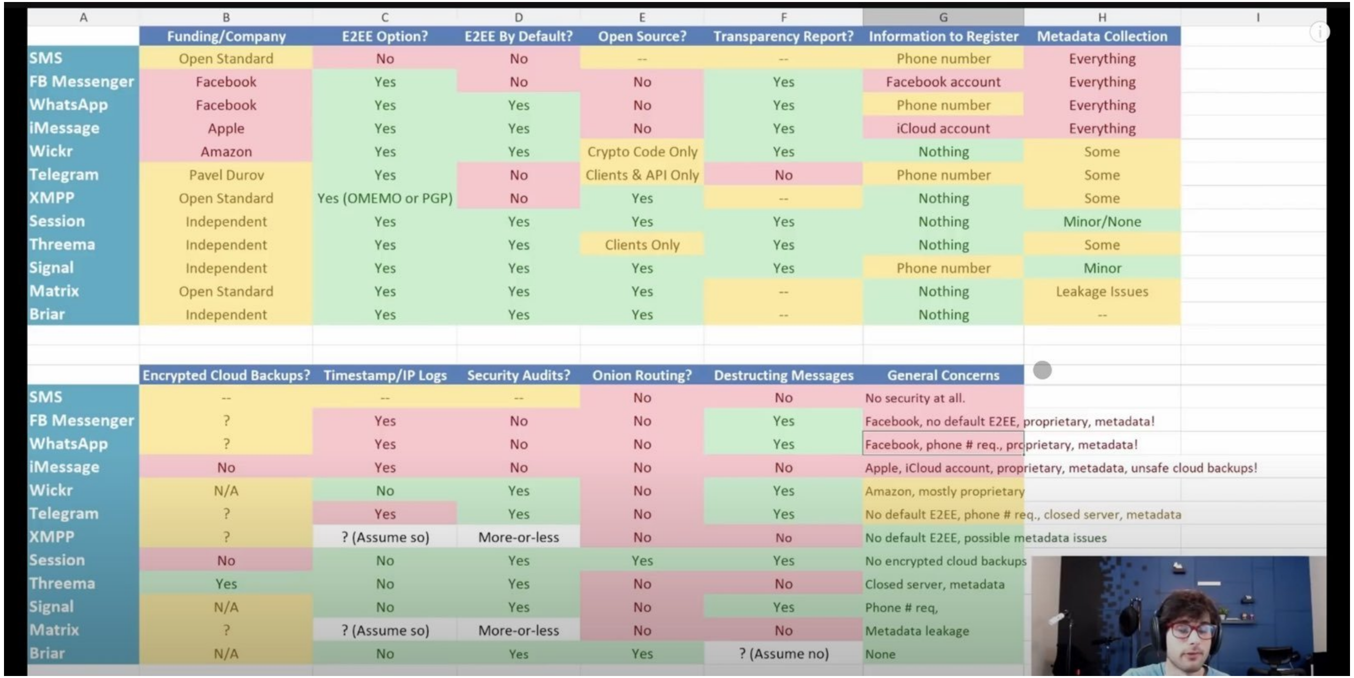
Capital letters (A-Z) ●

Include numbers (0-9) ●

Actionable Steps

- **Use a VPN (Mullvad, Proton Vpn)**
- **Stop Using Google Chrome (Brave, Firefox, Zen)**
- **Proton Mail instead of Gmail**
- **Use Linux instead of Windows, Pick a distro with https://distrochooser.de/**
- **Use a password manager (Proton Pass, Bitwarden)**
- **Use 2FA (Auth app, proton auth, ente auth)**
- **Google Drive alternatives: Cryptpad (for docs, sheets, etc.), Proton Drive**
- **Online meetings: Jitsi, Element**

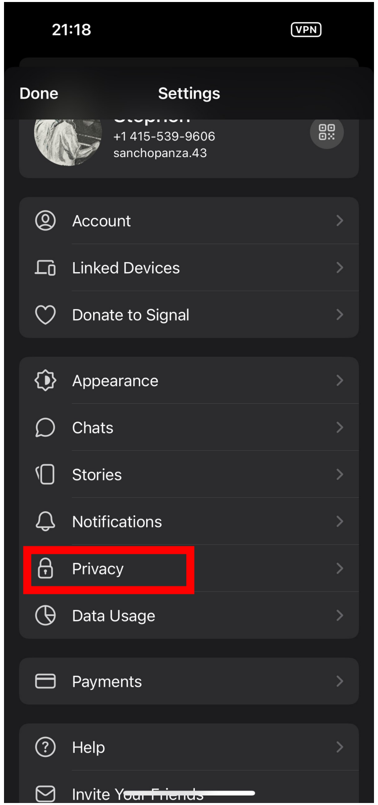
- **Stop using IMessages, Whatsapp or any proprietary messaging apps.**



	Funding/Company	E2EE Option?	E2EE By Default?	Open Source?	Transparency Report?	Information to Register	Metadata Collection
SMS	Open Standard	No	No	--	--	Phone number	Everything
FB Messenger	Facebook	Yes	No	No	Yes	Facebook account	Everything
WhatsApp	Facebook	Yes	Yes	No	Yes	Phone number	Everything
iMessage	Apple	Yes	Yes	No	Yes	iCloud account	Everything
Wickr	Amazon	Yes	Yes	Crypto Code Only	Yes	Nothing	Some
Telegram	Pavel Durov	Yes	No	Clients & API Only	No	Phone number	Some
XMPP	Open Standard	Yes (OMEMO or PGP)	No	Yes	--	Nothing	Some
Session	Independent	Yes	Yes	Yes	Yes	Nothing	Minor/None
Threema	Independent	Yes	Yes	Clients Only	Yes	Nothing	Some
Signal	Independent	Yes	Yes	Yes	Yes	Phone number	Minor
Matrix	Open Standard	Yes	Yes	Yes	--	Nothing	Leakage Issues
Briar	Independent	Yes	Yes	Yes	--	Nothing	--

	Encrypted Cloud Backups?	Timestamp/IP Logs	Security Audits?	Onion Routing?	Destructing Messages	General Concerns
SMS	--	--	--	No	No	No security at all.
FB Messenger	?	Yes	No	No	Yes	Facebook, no default E2EE, proprietary, metadata!
WhatsApp	?	Yes	No	No	Yes	Facebook, phone # req., proprietary, metadata!
iMessage	No	Yes	No	No	No	Apple, iCloud account, proprietary, metadata, unsafe cloud backups!
Wickr	N/A	No	Yes	No	Yes	Amazon, mostly proprietary
Telegram	?	Yes	Yes	No	Yes	No default E2EE, phone # req., closed server, metadata
XMPP	?	? (Assume so)	More-or-less	No	No	No default E2EE, possible metadata issues
Session	No	No	Yes	Yes	Yes	No encrypted cloud backups
Threema	Yes	No	Yes	No	No	Closed server, metadata
Signal	N/A	No	Yes	No	Yes	Phone # req,
Matrix	?	? (Assume so)	More-or-less	No	No	Metadata leakage
Briar	N/A	No	Yes	Yes	? (Assume no)	None

Signal Phone Number Removal



21:18 VPN

Done Settings

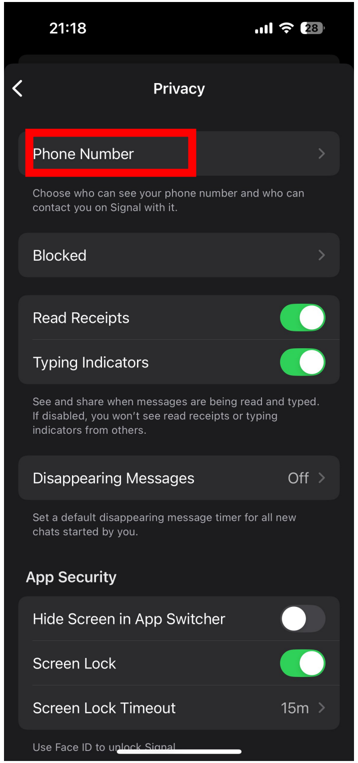
Stephen
+1 415-539-9606
sanchopanza.43

Account
Linked Devices
Donate to Signal

Appearance
Chats
Stories
Notifications
Privacy
Data Usage

Payments

Help
Invite Your Friends



21:18 28

Privacy

Phone Number

Choose who can see your phone number and who can contact you on Signal with it.

Blocked

Read Receipts
Typing Indicators

See and share when messages are being read and typed. If disabled, you won't see read receipts or typing indicators from others.

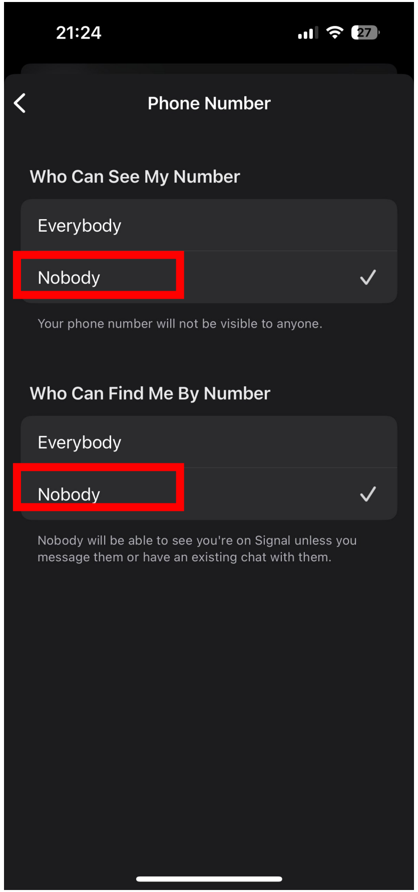
Disappearing Messages Off

Set a default disappearing message timer for all new chats started by you.

App Security

Hide Screen in App Switcher
Screen Lock
Screen Lock Timeout 15m

Use Face ID to unlock Signal



21:24 27

Phone Number

Who Can See My Number

Everybody
Nobody ✓

Your phone number will not be visible to anyone.

Who Can Find Me By Number

Everybody
Nobody ✓

Nobody will be able to see you're on Signal unless you message them or have an existing chat with them.

In General only use open source and federated software unless absolutely necessary

Find here: https://alternativeto.net/

When Going Somewhere...

- **Go with a buddy or group**
- **Wear a mask and non-identifiable clothing**
- **Ideally use a burner or old phone**
- **Turn off biometric security (fingerprint, face, etc.)**
- **On BART, Use a non-digital wallet, non-school affiliated Clipper card, paid in cash**
- **If detained Power Off Phone**

EVERY ACTION NOW IS A HIGH RISK ACTION

Digital Cleanliness and Good Practice

- Don't need it? Delete It!
- If in chats with people whose phones were confiscated:
  - Remove them from chats
  - Leave & delete chats
  - Change Signal Username
- Don’t connect to public wi-fi networks (without VPN)
- Don’t click on unknown/expected links, downloads, etc.
- Wipe Thoroughly and Often
- Be Mindful of Social Media
- Be mindful of public likes, reposts, etc.
- Try to migrate off of Big Tec Social Media Platforms

Digital Security is not just for you, it’s for everyone you work with and interact with.

If one person is vulnerable, all of us are vulnerable.

Questions

- **Ask @sanchopanza.43 on signal**