Resistencia Digital

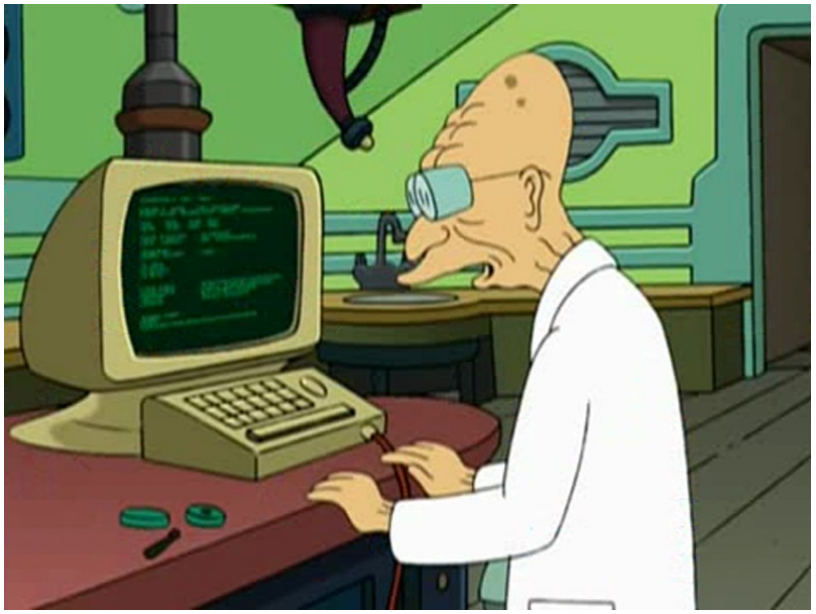
Seguridad y privacidad en la era Smartphone

Carlos Fernández
NcN 2019

Presentación

Carlos Fernández

- Ingeniero de Telecos
- Red Teamer
- Miembro de Críptica
- Coautor del libro *Resistencia Digital: Manual de seguridad operacional e instrumental para smartphones*



Presentación

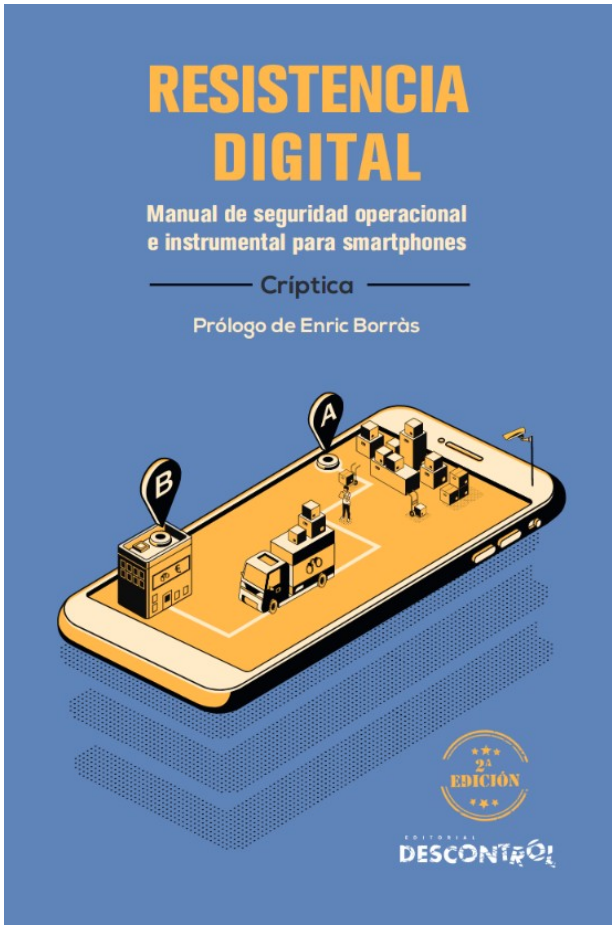
Críptica

- Fundada en 2015
- Asociación en defensa de la privacidad
- Intentamos acercar hábitos y tecnologías seguras a la sociedad

Presentación

Resistencia Digital

- Manual de seguridad para smartphones
- Publicado en abril de 2019
- Gratis en versión digital desde septiembre!



https://www.criptica.org/material/resistencia_digital.pdf

Vigilancia masiva

Privacidad

”No tengo nada que esconder”

Privacidad

Ideas (erróneas) tras la frase:

- Sólo los ”malos” tienen cosas que esconder
- Yo no soy nadie ni estoy haciendo nada malo

Realidad:

- Para el poderoso, aquel que le desafía es malo también. Periodistas, activistas…
- No sabes cómo te afectará mañana la información que generas hoy.
- Derecho a la intimidad

Intimidad

Tenemos derecho a una vida privada

- ¿Por qué no vives en una casa de cristal?
- ¿Por qué cierras el pestillo del baño?
- ¿Por qué no me dejas conocer tus problemas personales, amorosos o familiares?
- ¿Por qué no me dejas leer tus mensajes y compartir públicamente los que yo quiera?

- **¿Acaso tienes algo que esconder?**

Privacidad como garante de otros derechos

La vigilancia condiciona nuestras libertades:

- Comportamiento
- Reunión
- Asociación
- Expresión
- Pensamiento

¿Nada que ocultar?

"Decir que no te preocupa la privacidad porque no tienes nada que ocultar es como decir que no te preocupa la libertad de expresión porque no tienes nada que decir".

E. Snowden

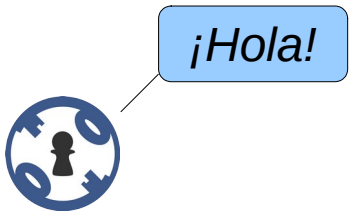
¿Cómo defenderse?

security in-a-box
caja de herramientas de seguridad
protegiendo tu privacidad digital

LA QUADRATURE DU NET

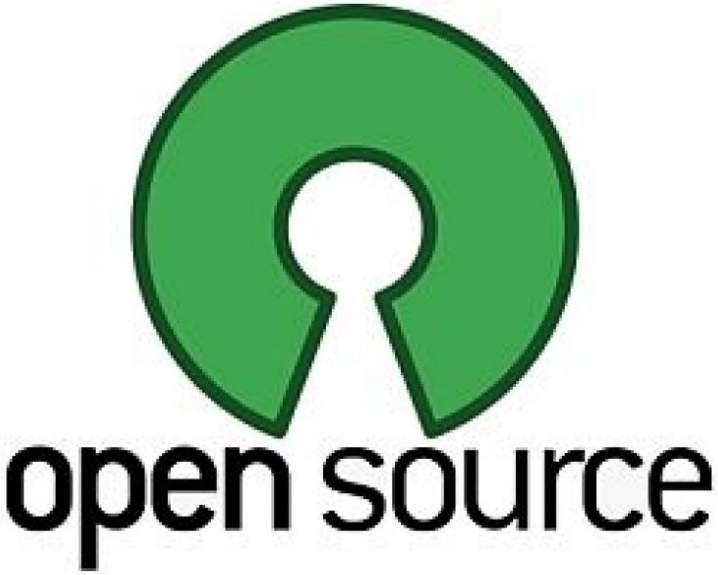
ELECTRONIC FRONTIER FOUNDATION

privacytools.io



Código abierto

Las herramientas de código abierto permiten que el funcionamiento real de la herramienta sea auditable por la comunidad

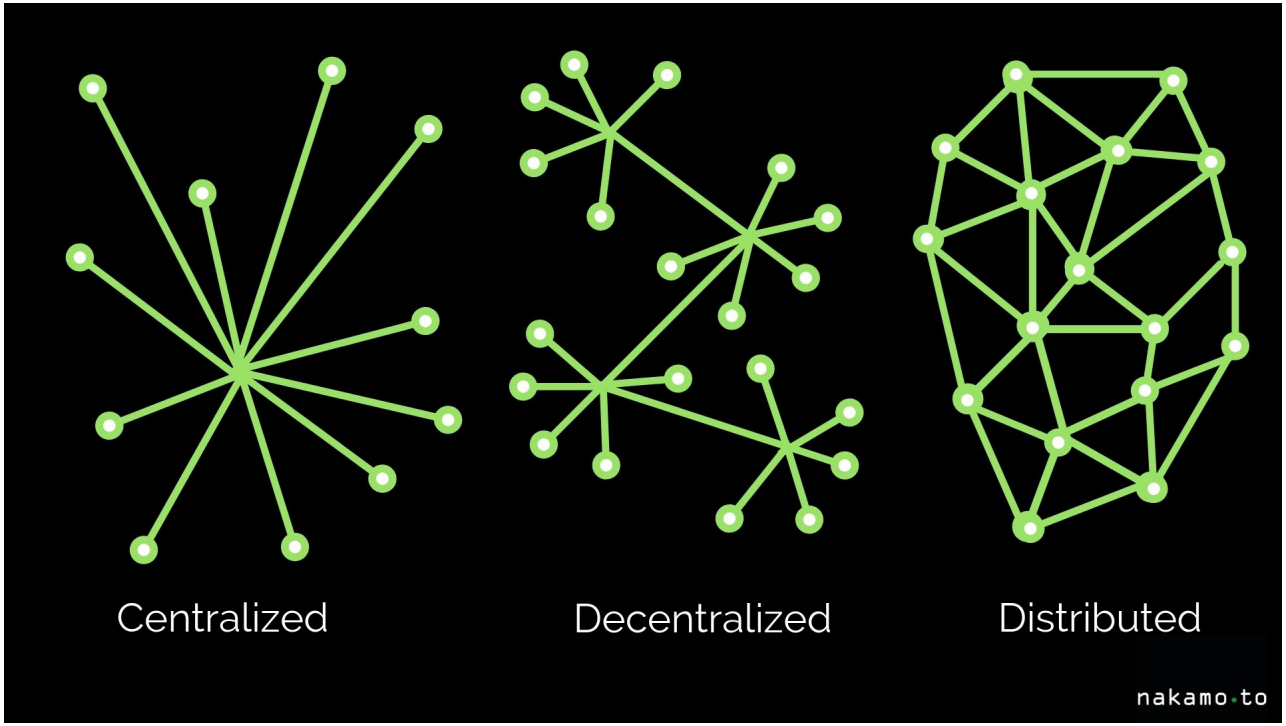


Privacidad por diseño

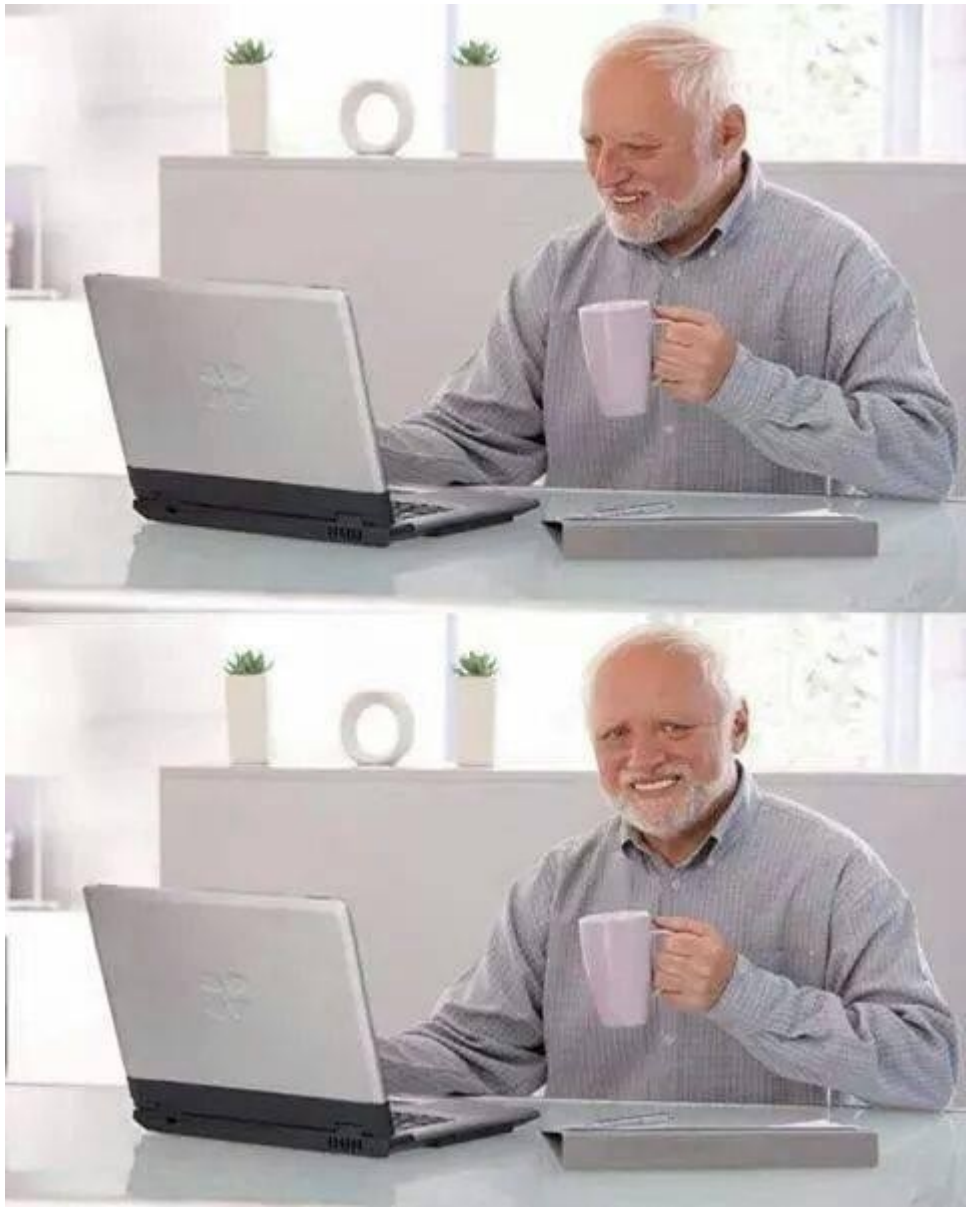
Privacidad garantizada por diseño, no por política: Cifrado extremo a extremo, uso de los datos personales mínimos imprescindibles, protección del anónimato...

Descentralización

La información no puede estar en manos de un único proveedor



Usabilidad



La privacidad debe de estar al alcance de todo el mundo y no depender de un hipotético conocimineto experto del usuario.

Modelado adversarial

Seguridad operacional

Para mantener una conversación privada...

- Seguridad instrumental: cifrado extremo a extremo, código abierto, comunicación distribuida...

- Seguridad operacional: ¿Confías en tu interlocutor?¿Hay alguien mirando por encima del hombro?¿Debería guardar esta información en mi dispositivo?

El dispositivo Smartphone

Poco favorable a la protección de la privacidad:

- Centralización de mucha información en un solo dispositivo
- Áltamente íntimo y con gran cantidad de sensores
- Ecosistema de aplicaciones invasivas
- Favorece el uso de servicios centralizados
- Siempre encendido, siempre encima y siempre localizado

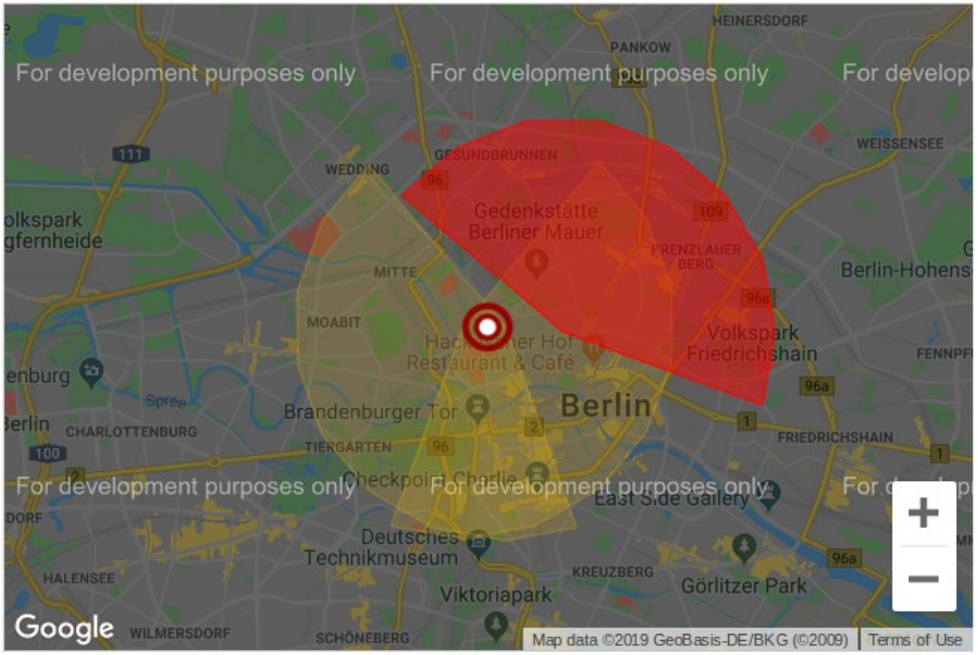
Red de telefonía

Por el mero hecho de usar un teléfono móvil, tu proveedor conoce:

- Tu localización aproximada
- A quién llamas, cuando y durante cuanto rato
- Con quien intercambias SMS
- Qué sitios web visitas, o qué protocolos usas
- Tiene la capacidad técnica de inspeccionar todo lo que no esté cifrado

https://www.zeit.de/datenschutz/malte-spitz-data-retention

Retención de datos



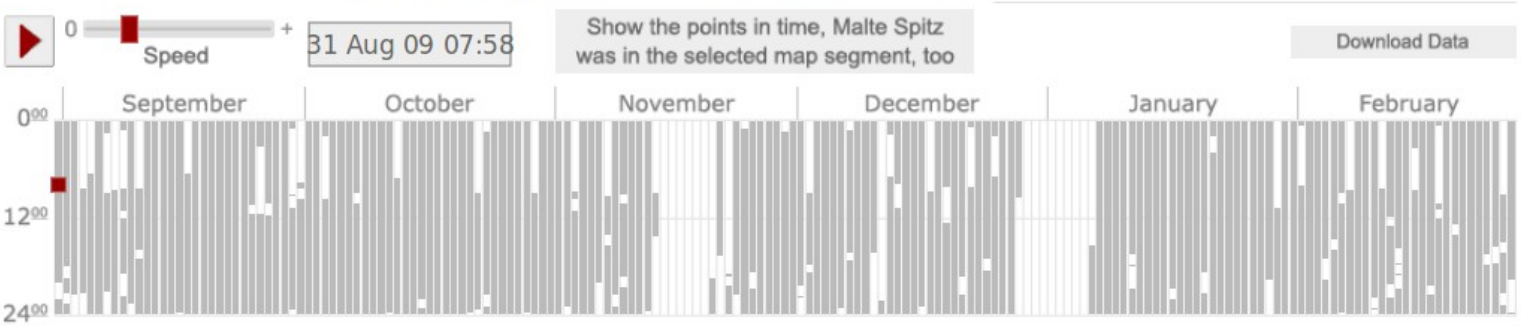
Monday, 31 August 2009

Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.
(source: Parteiwebsite)

6 incoming calls
21 outgoing calls
total time: 1h 16min 8s

34 incoming messages
29 outgoing messages

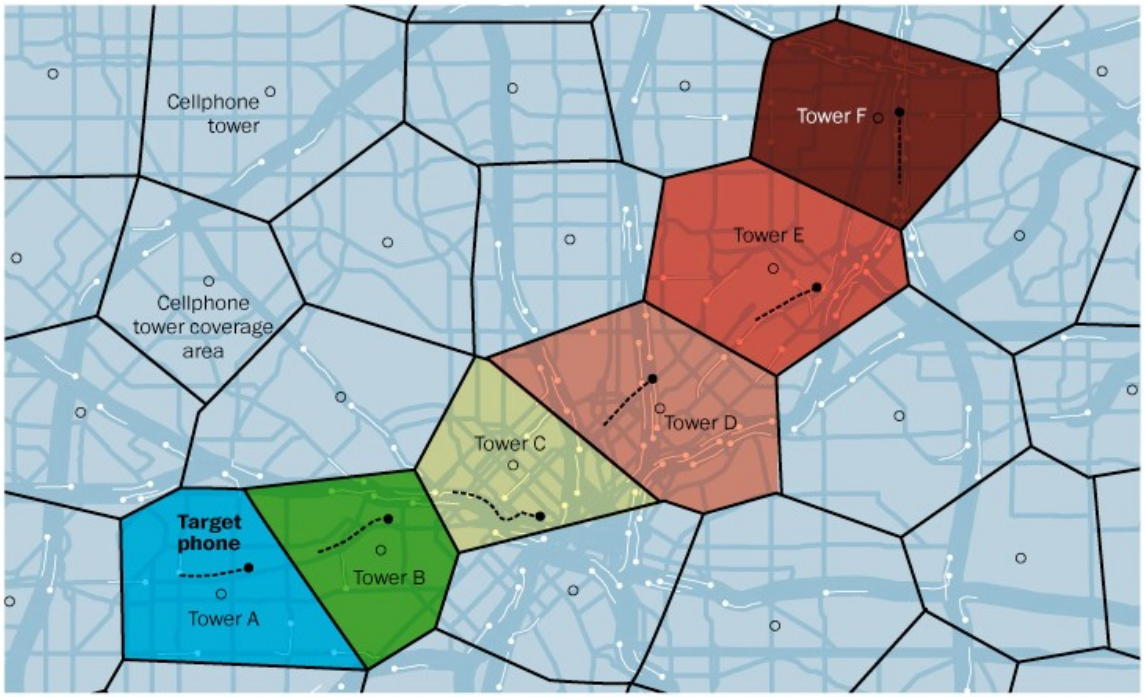
duration of internet connection:
21h 17min 25s



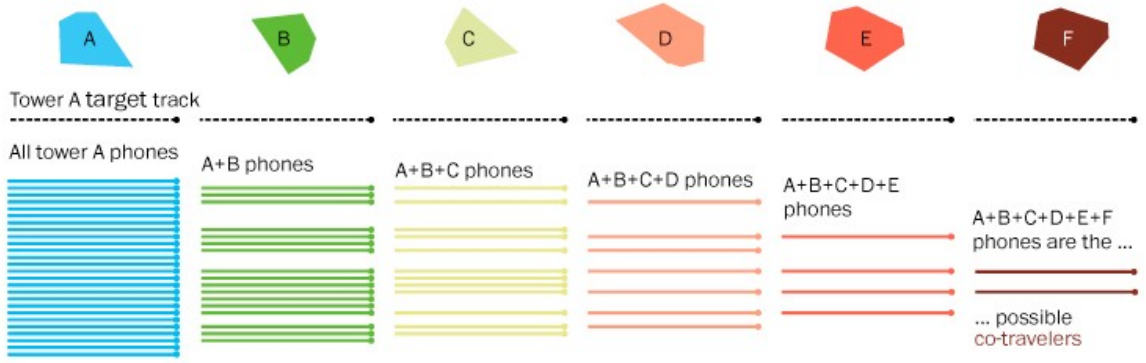
https://www.zeit.de/datenschutz/malte-spitz-data-retention

Combinación de datos

By tracking all phones within a cell tower area along with the target phone, co-travelers can be isolated.



As the target phone moves from tower to tower, fewer and fewer potential co-travelers remain.



Protección de la privacidad

La fiebre de las apps

Info que puede recopilar una web

- Dirección IP
- Navegador
- Sistema operativo
- Idioma del navegador
- Cookies: Correlación con actividad previa o futura
- Monitorización de la avtividad en el sitio web.
- Información que hayamos introducido explícitamente.

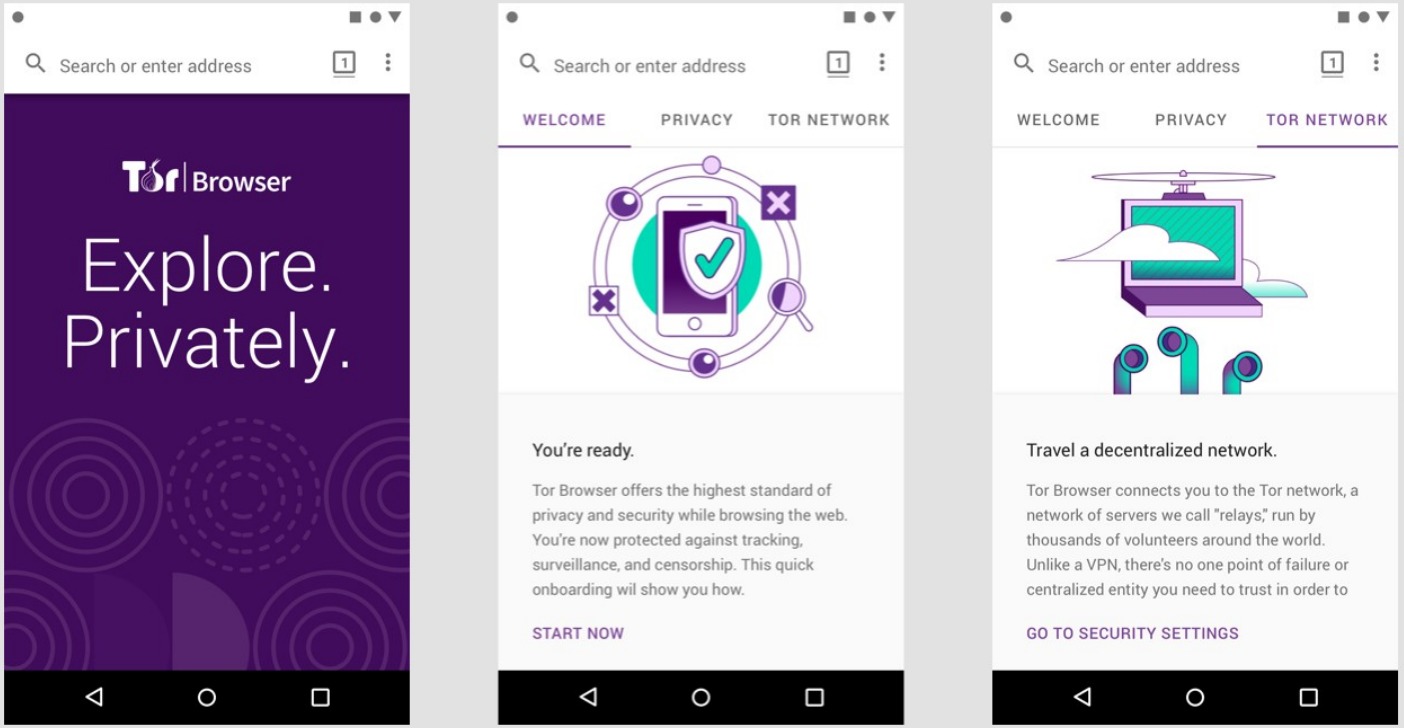
Firefox y Complementos de Navegación

- Firefox incorpora bloqueo de rastreadores de tereceros desde principios de septiembre

- Ublock Origin
- Privacy Badger
- Cookie Autodelete
- HTTPS Everywhere

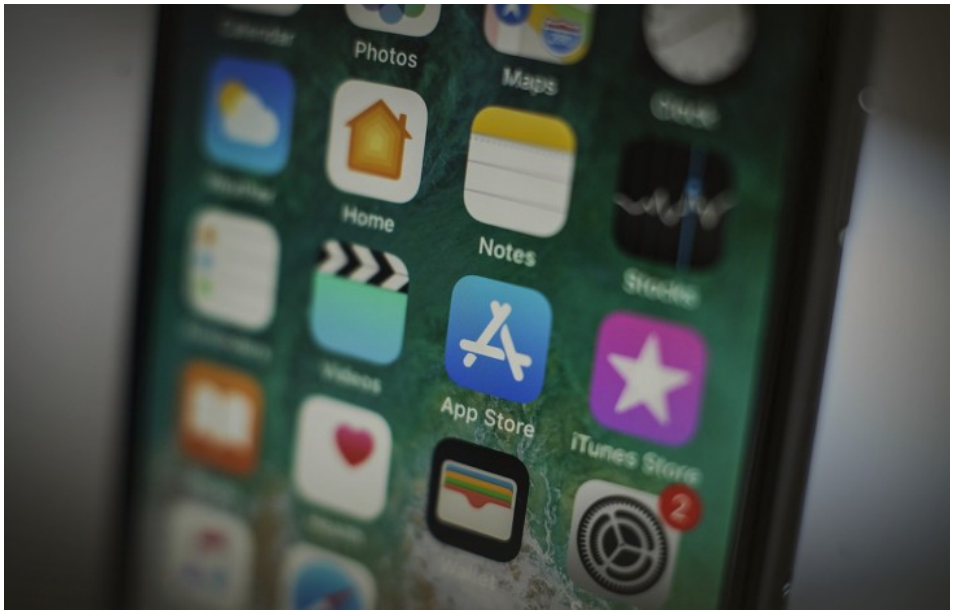



Anonimato con Tor browser



Info que puede recopilar una app

- Identidad
- Contactos
- Calendario
- Información de Wi-Fi
- Localización GPS
- SMS
- Llamadas
- Micrófono
- Cámara
- Archivos
- ...

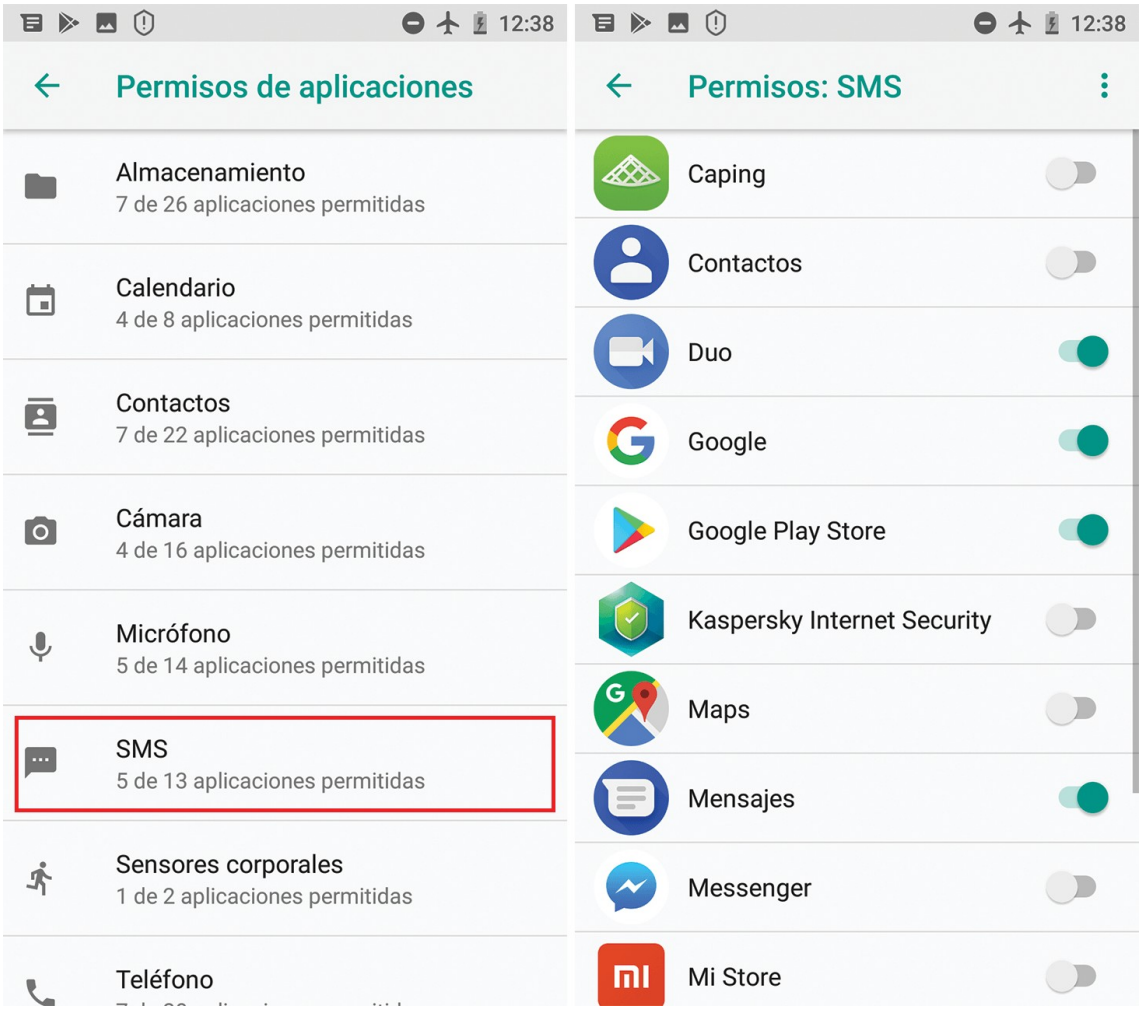


Sentido común + apps respetuosas

Preguntas que nos pueden ayudar:

- ¿Es necesario que me instale esta app?
- ¿Estoy de acuerdo con los permisos que me pide?
- ¿Existe alguna alternativa más respetuosa con mi privacidad?
- https://privacytools.io
- https://prism-break.org
- Página 115 de *Resistencia Digital*

Control de permisos (Android)

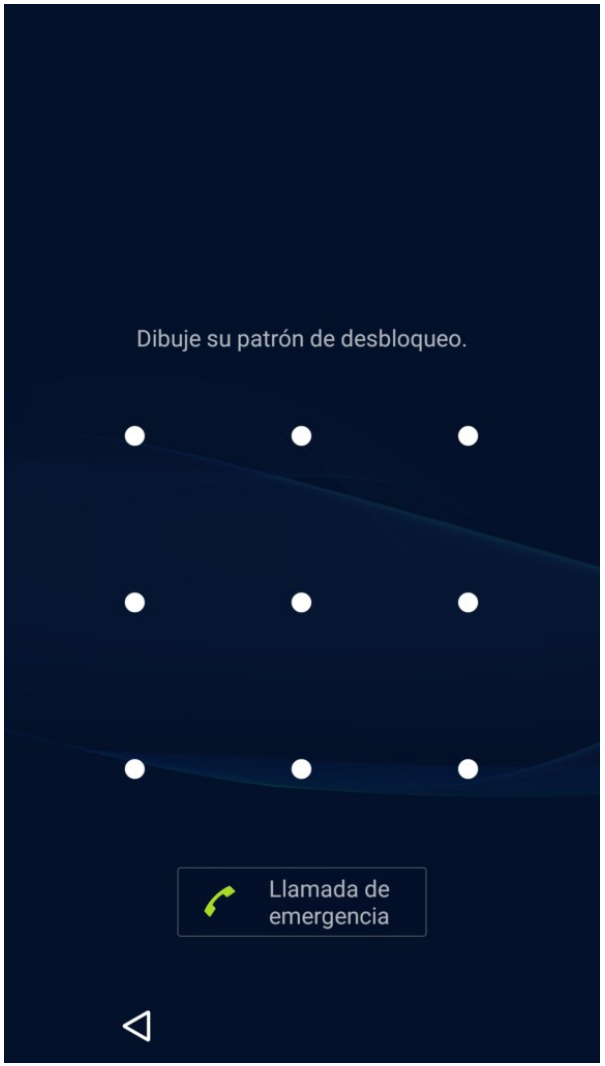


Control de permisos (iOS)

Protección frente al acceso físico

Desbloqueo seguro

Desbloqueo seguro: Patrón



Consiste en deslizar el dedo, uniendo los puntos.

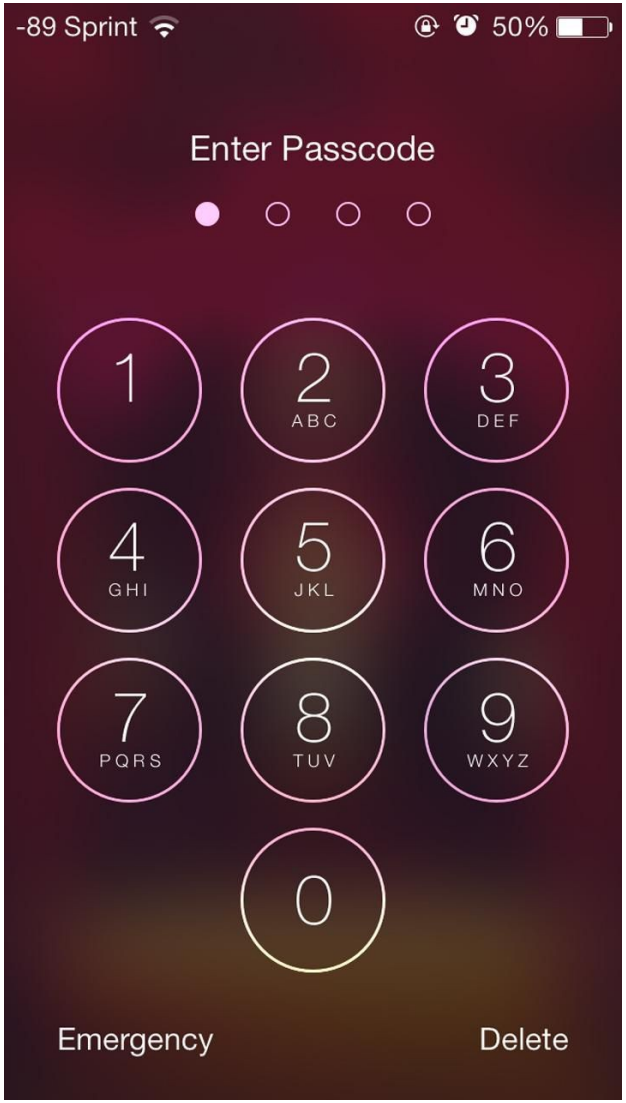
A favor:

- Usable
- Fácil de recordar

En contra

- Las trazas de los dedos en la pantalla
- Fácil de ver y recordar por encima del hombro
- Alfabeto reducido (9 puntos) y no se pueden repetir

Desbloqueo seguro: Pin



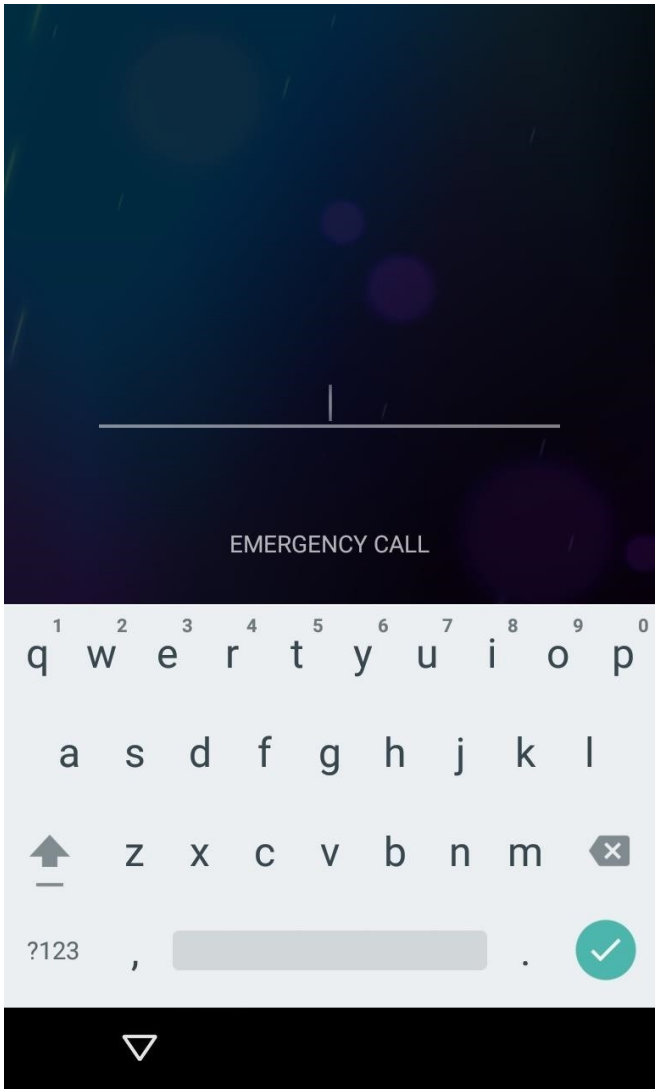
A favor:

- Usable
- Fácil de recordar

En contra

- Fácil de ver y recordar por encima del hombro, si es corto
- Alfabeto reducido (10 dígitos) y no se pueden repetir. Lo podemos compensar con un pin largo (10 cifras)

Desbloqueo seguro: Contraseña



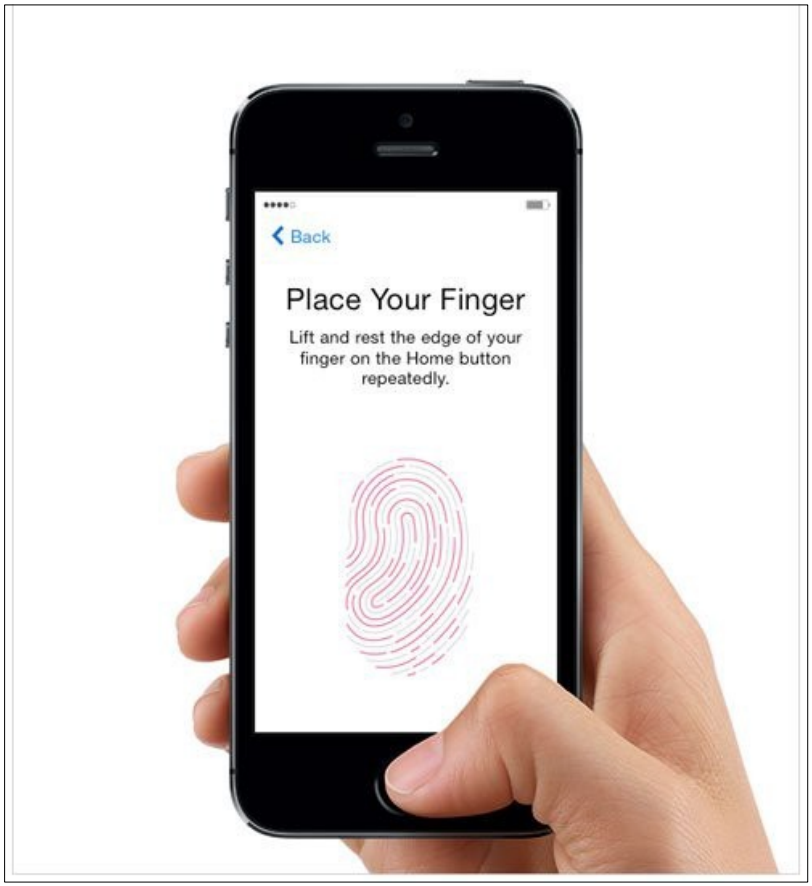
A favor:

- Permite una mayor complejidad (mayor alfabeto)
- Más difícil de ver que el pin o el patrón

En contra:

- Menos usable: se tarda más en introducirla
- Más facilidad de cometer errores.

Desbloqueo seguro: Biometría



Consiste en desbloquear el teléfono usando rasgos físicos (huella, cara, iris).

A favor:

- Usable (rápida y difícil equivocarse)

En contra

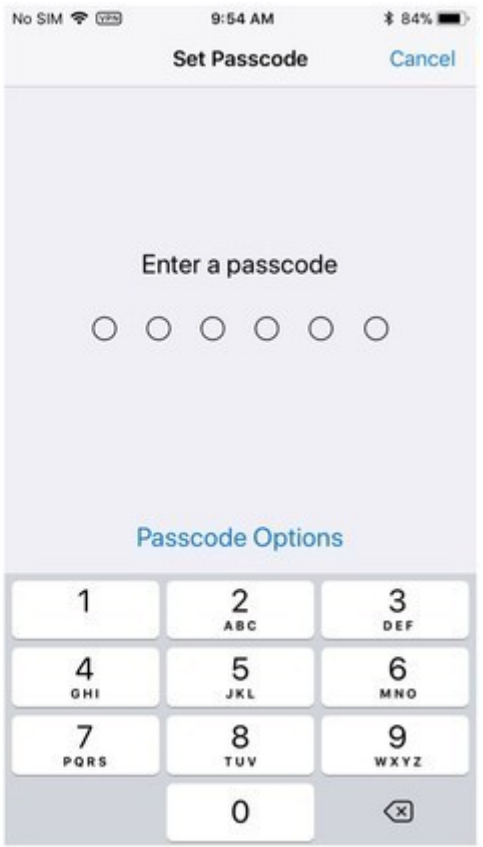
- Inútil si el adversario puede reproducirla o forzarnos a introducirla.
- La biometría no es revocable.

Cifrado de memoria

Protección de la información guardada en el teléfono.

Incluso si se copia la memoria del teléfono con un dispositivo especializado, la información no podrá ser accedida sin la clave de cifrado.

Cifrado de memoria: iOS

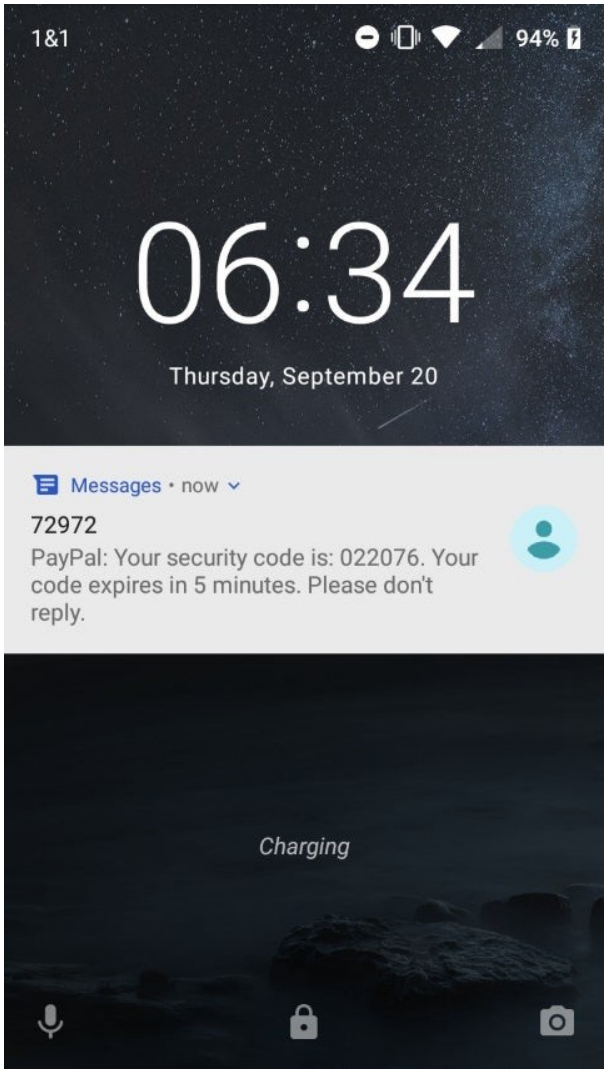


https://www.imore.com/passcode

Cifrado de memoria: Android

https://elandroidelibre.elespanol.com/2019/03/como-encriptar-microsd-telefono-android.html

Previsualización de notificaciones



Protección frente al acceso remoto

Origen de las aplicaciones: Android

Por defecto sólo permite Google Play

Se puede habilitar ”orígenes desconocidos” desde el menú de ajustes.

Esto permite instalar aplicaciones de código abierto desde F-Droid.

Cuidado con otras tiendas alternativas y enlaces de descarga de apps recibidos por mensaje!

Sentido común y apps respetuosas

Origen de las aplicaciones: iOS

Permite sólo desde la AppStore, excepto si hacemos *Jailbreak* o con licencia de desarrollador.

Filosofía cerrada: Resta libertad al usuario.

Más difícil que un atacante instale malware.

Sentido común y apps respetuosas

¡Actualizad malditos!

Tanto apps como sistema operativo

Nos protege de posibles vulnerabilidades.

¡Actualizad malditos!

WhatsApp vulnerability exploited through malicious GIFs to hijack chat sessions

ZDNet

Personal files and messages are at risk in unpatched builds of the app.

By Charlie Osborne for Zero Day | October 3, 2019 -- 10:45 GMT (11:45 BST) | Topic: Security

ars TECHNICA

REINING IN THE WILD WEST —

WhatsApp suit says Israeli spyware maker exploited its app to target 1,400 users

Clickless exploit targeted attorneys, journalists, activists, dissidents, and others.

DAN GOODIN - 10/29/2019, 11:40 PM

Contraseñas

Las contraseñas son como la ropa interior

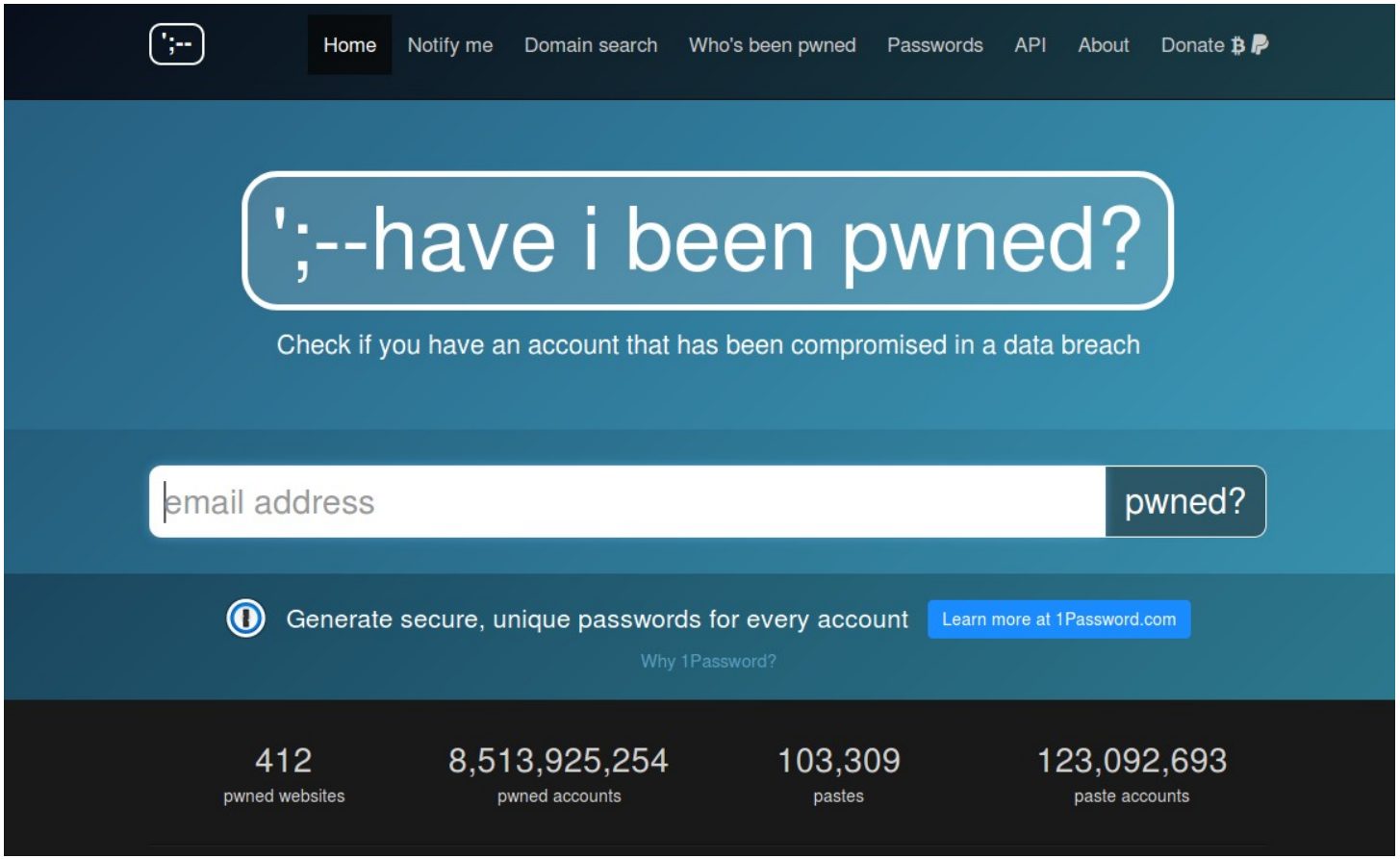
- No las reutilices
- No las compartas
- No las dejes a la vista

Consejos:

Una contraseña es mas compleja cuánto más larga es: Utiliza frases o combina palabras al azar.

Utiliza un gestor de contraseñas como KeepassX (Escritorio) o KeepassDroid (Android).

Brechas de seguridad



Two-Factor Authentication (2FA)

- Protección adicional
- Pérdida del posible anonimato

https://blog.malwarebytes.com/101/2018/09/two-factor-authentication-2fa-secure-seems/

Comunicación segura: Navegación

- HTTPS permite verificar el servidor al que nos conectamos
- HTTPS proporciona un canal cifrado con el servidor

Es muy importante asegurarse de que el dominio es correcto! (mibanco.com vs mibacno.com)

Mensajería segura: Criterios

- **Cifrado extremo a extremo:** Sólo los interlocutores pueden ver los mensajes, la comunicación está protegida de modo que el proveedor no puede leerlos.

- **Autoborrado de mensajes:** Los mensajes pueden ser programados para ser borrados automáticamente un tiempo despues de ser leídos

- **Disponibilidad del código:** El código fuente está publicado.

Mensajería segura: Criterios

- **Identificación mediante el número de teléfono:** La aplicación de mensajería necesita el número de teléfono para funcionar

- **Número de teléfono expuesto:** El interlocutor conocerá tu número de teléfono

Mensajería segura: Criterios

- **Arquitectura:** Puede ser centralizada, descentralizada (federada) o distribuida (P2P).

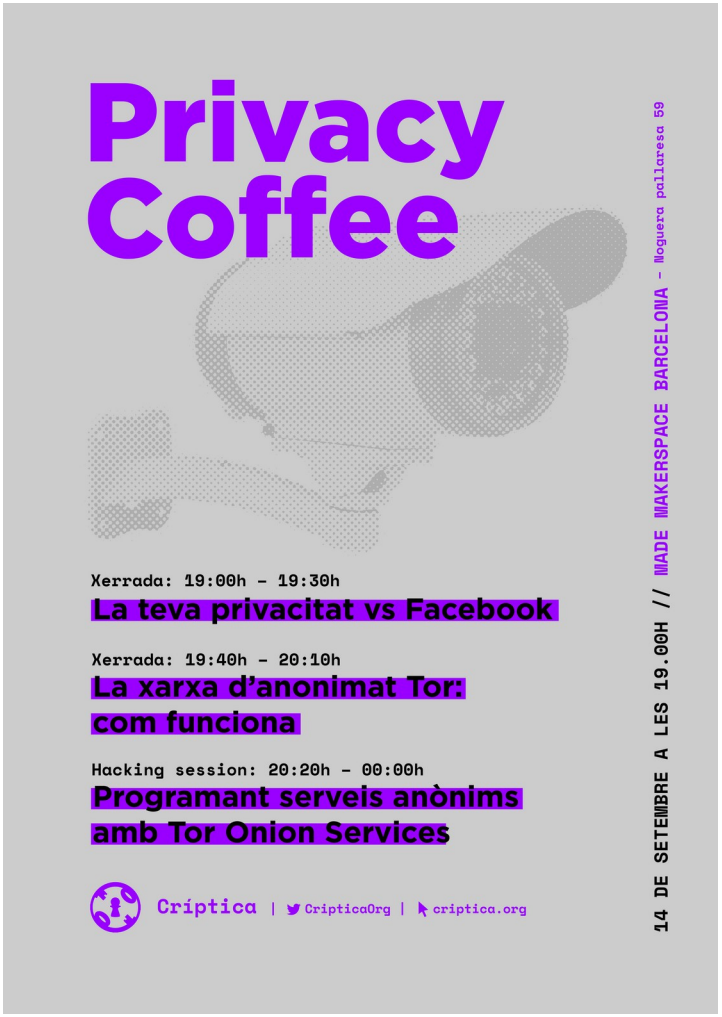
- **Modelo de negocio:** Puede ser con ánimo de lucro y basado en datos de usuario, sin ánimo de lucro, o con ánimo de lucro basado en suscripciones de pago.

Comunicación segura: Mensajería

APLICACIÓN	CIFRADO E2E	AUTOBORRADO DE MENSAJES	IDENTIFICACIÓN CON NÚMERO DE TELÉFONO	NÚMERO DE TELÉFONO EXPUESTO	ARQUITECTURA	DISPONIBILIDAD DEL CÓDIGO	MODELO DE NEGOCIO
SMS	NO	NO	SÍ	SÍ	CENTRALIZADA	-	EMPRESA
WHATSAPP	SÍ	NO	SÍ	SÍ	CENTRALIZADA	NO	EMPRESA PROPIEDAD DE FACEBOOK INC.
TELEGRAM	Sólo en los chats secretos (no aplicable en grupos)	Sólo en los chats secretos habilitado manualmente	SÍ	APLICACIÓN	CENTRALIZADA	SÍ	EMPRESA
SIGNAL	SÍ	SÍ, aunque debe ser habilitado manualmente	SÍ	SÍ	CENTRALIZADA	SÍ	FUNDACIÓN SIN ÁNIMO DE LUCRO
WIRE	SÍ	NO	No necesaria en caso de activar la cuenta a través de la web	NO	CENTRALIZADA	SÍ	EMPRESA
MATRIX (RIOT)	SÍ, aunque debe ser habilitado manualmente	NO	No necesaria	NO	SISTEMA FEDERADO	SÍ	FUNDACIÓN SIN ÁNIMO DE LUCRO

Comunidad

Eventos periódicos en Barcelona:



Contacto

- Web: https://criptica.org
- Matrix: https://matrix.to/#/#criptica:matrix.org
- Twitter: @CripticaOrg
- Mail: info [at] criptica.org