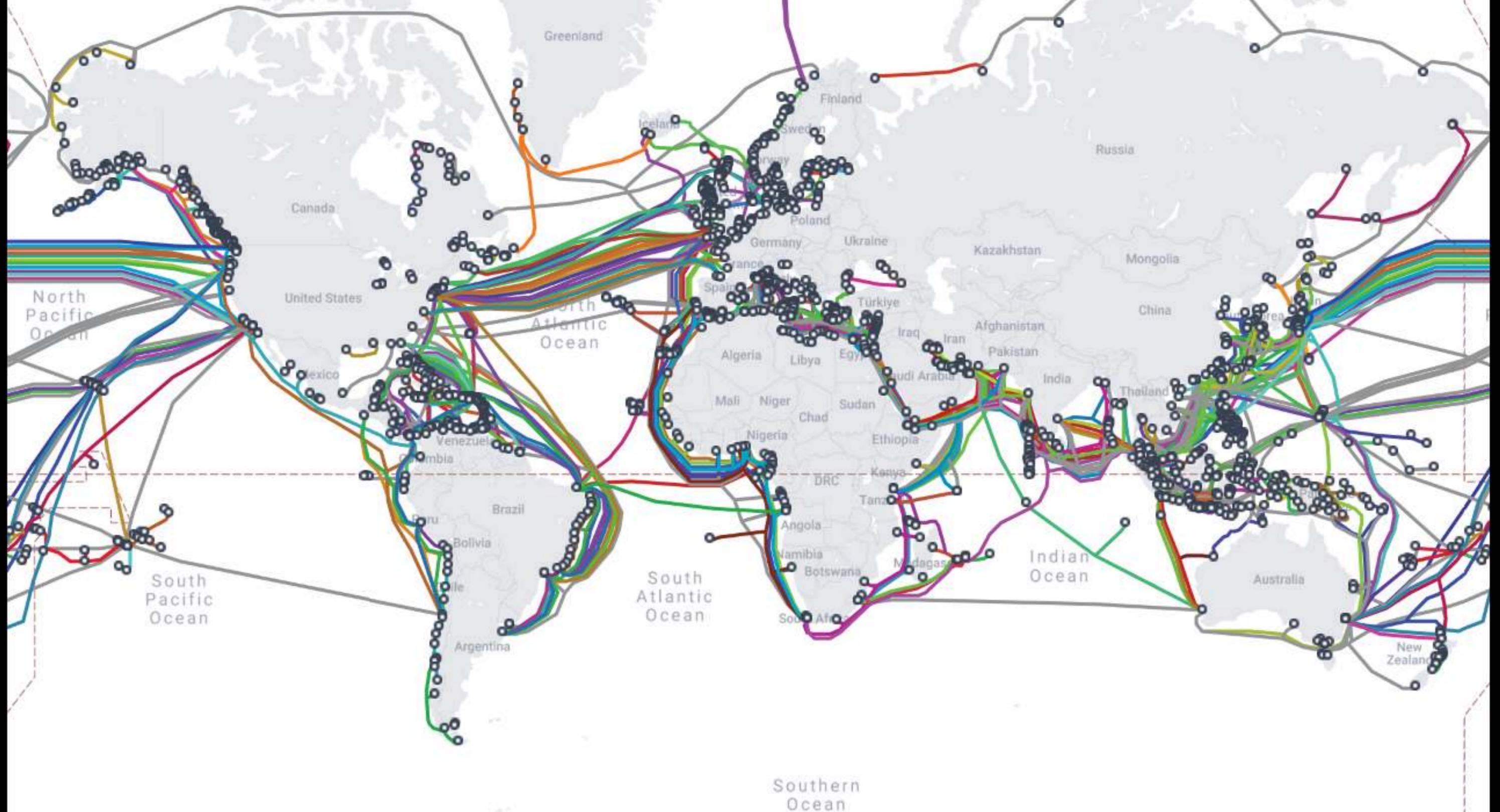


CUIDADOS DIGITALES

**Cuidándonos de manera colectiva
en el internet**

1- Interconectados o el Internet de las Cosas

INTERCONNECTIVIDAD



INTERCONECTIVIDAD



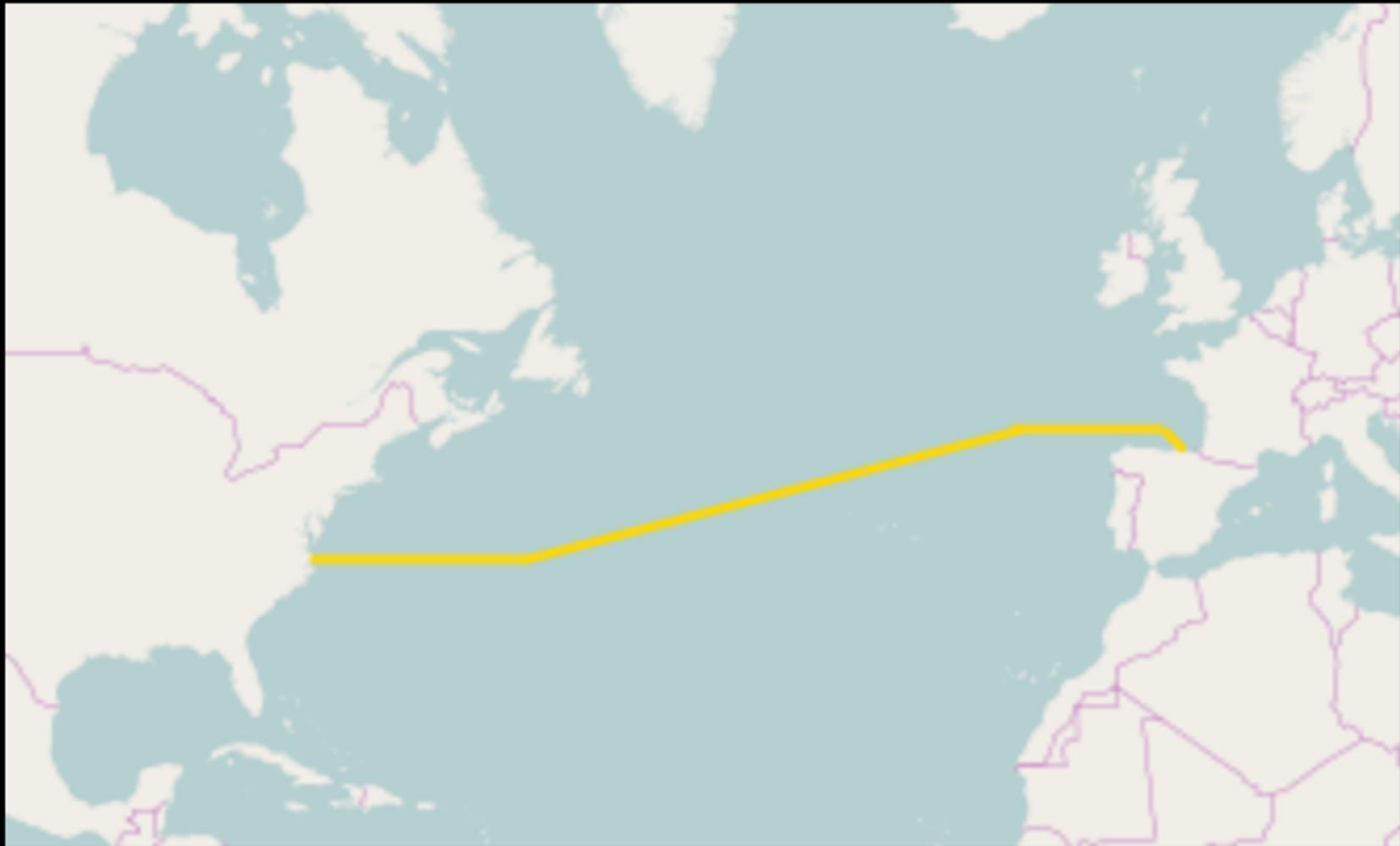
Alrededor de más de
1 millón de kilómetros a 2025

En 2012 las bigtech
eran dueñas del 10%
actualmente es casi el 70%





Proyecto Marea
6,600 km
de Virginia a España



Earth Submarine Fiber Optic Cable Network

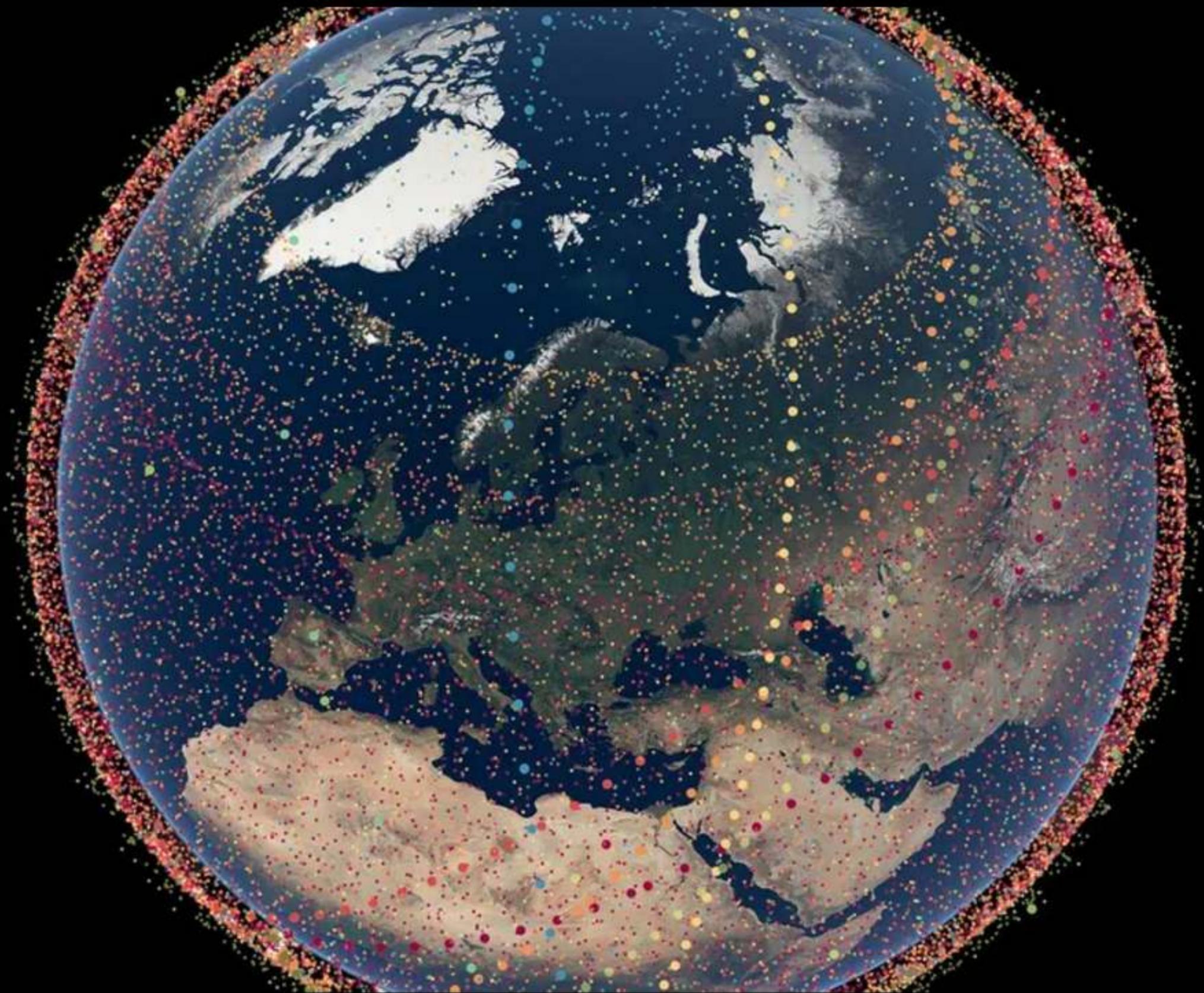
Network Stylized for Clarity—Actual Physical Routes Not Shown



Created with rayrender (www.rayrender.net)

Data: github.com/telegeography/www.submarinecablemap.com

Twitter: [@tylormorganwall](https://twitter.com/tylormorganwall)

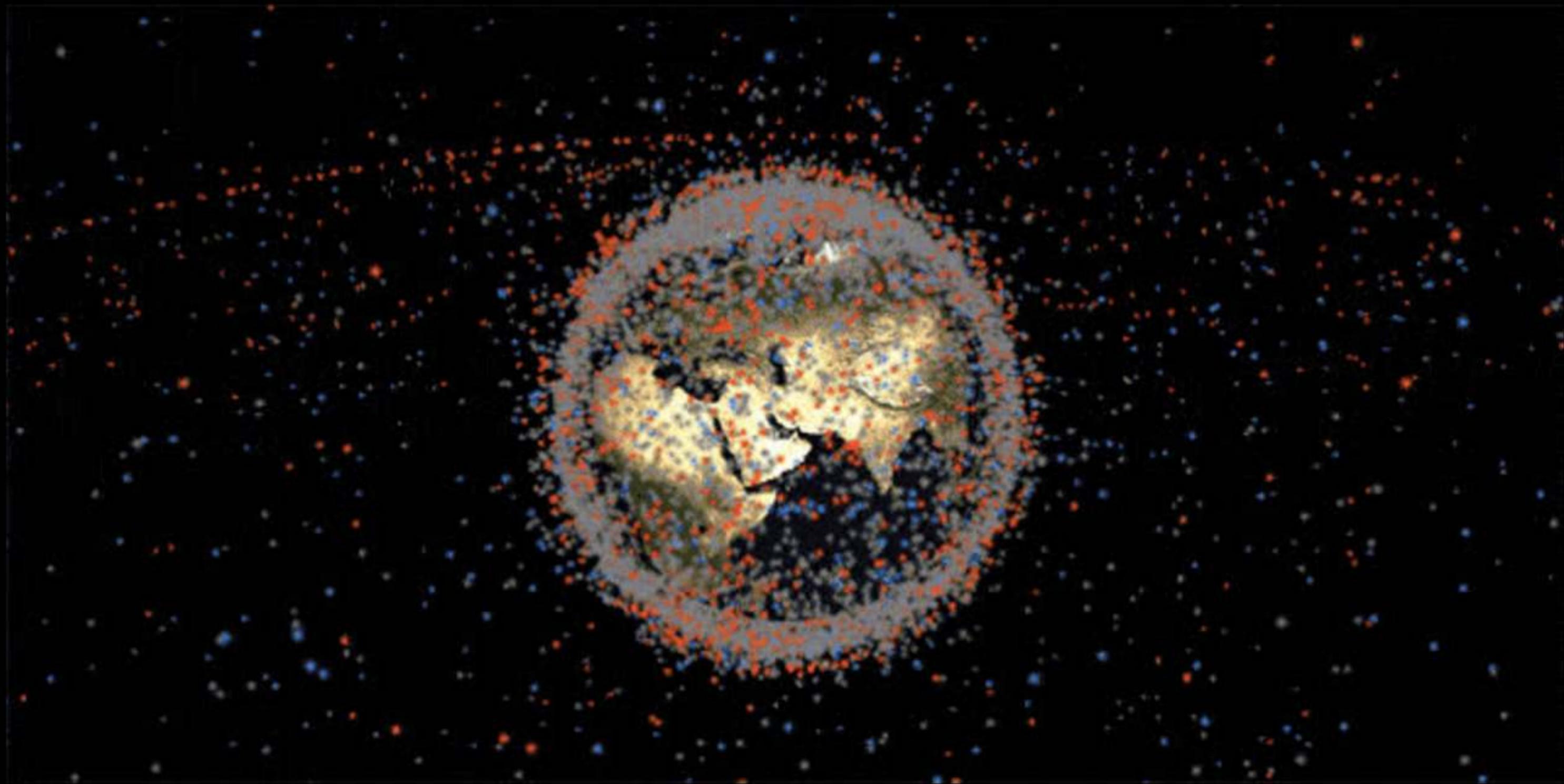




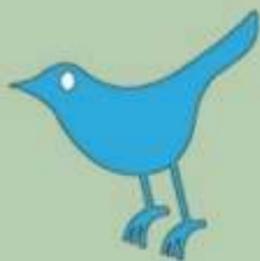
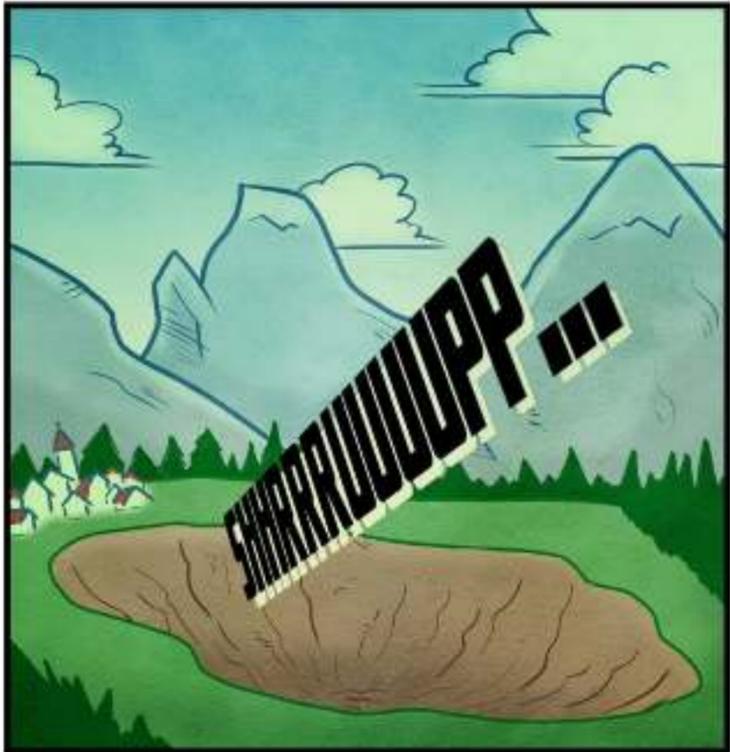
Los satélites Starlink orbitan a unos 550 kilómetros de distancia de la Tierra. Esta distancia es significativamente menor que la de los satélites geoestacionarios tradicionales, que orbitan a aproximadamente 35 786 kilómetros

<https://satellitemap.space/>

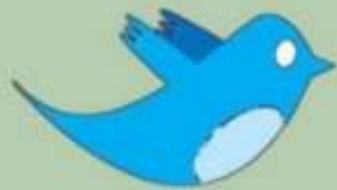
<https://satmap.space/>



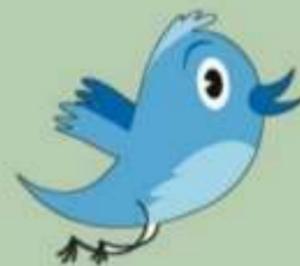
POCOS GULAGS HAY



2006



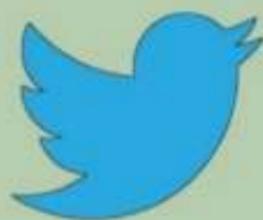
2007



2009



2010



2012



2023



2025

Tecnología · Más Tecnología

La República Democrática del Congo demanda a Apple por usar “minerales de sangre”



**2- ¿De qué y de quién
nos cuidamos?**

¿De quienes nos cuidamos?

En la ciberseguridad se le llama agente malicioso, agente de intrusión, atacante, a quienes ocupan esas vulnerabilidades y amenazas del internet.
Hay quienes confunden el termino HACKER con el de ciber criminal.

HACKER experimenta y descubre

CIBERCRIMINAL atenta contra las regulaciones del internet

SOCIEDAD DE LA VIGILANCIA

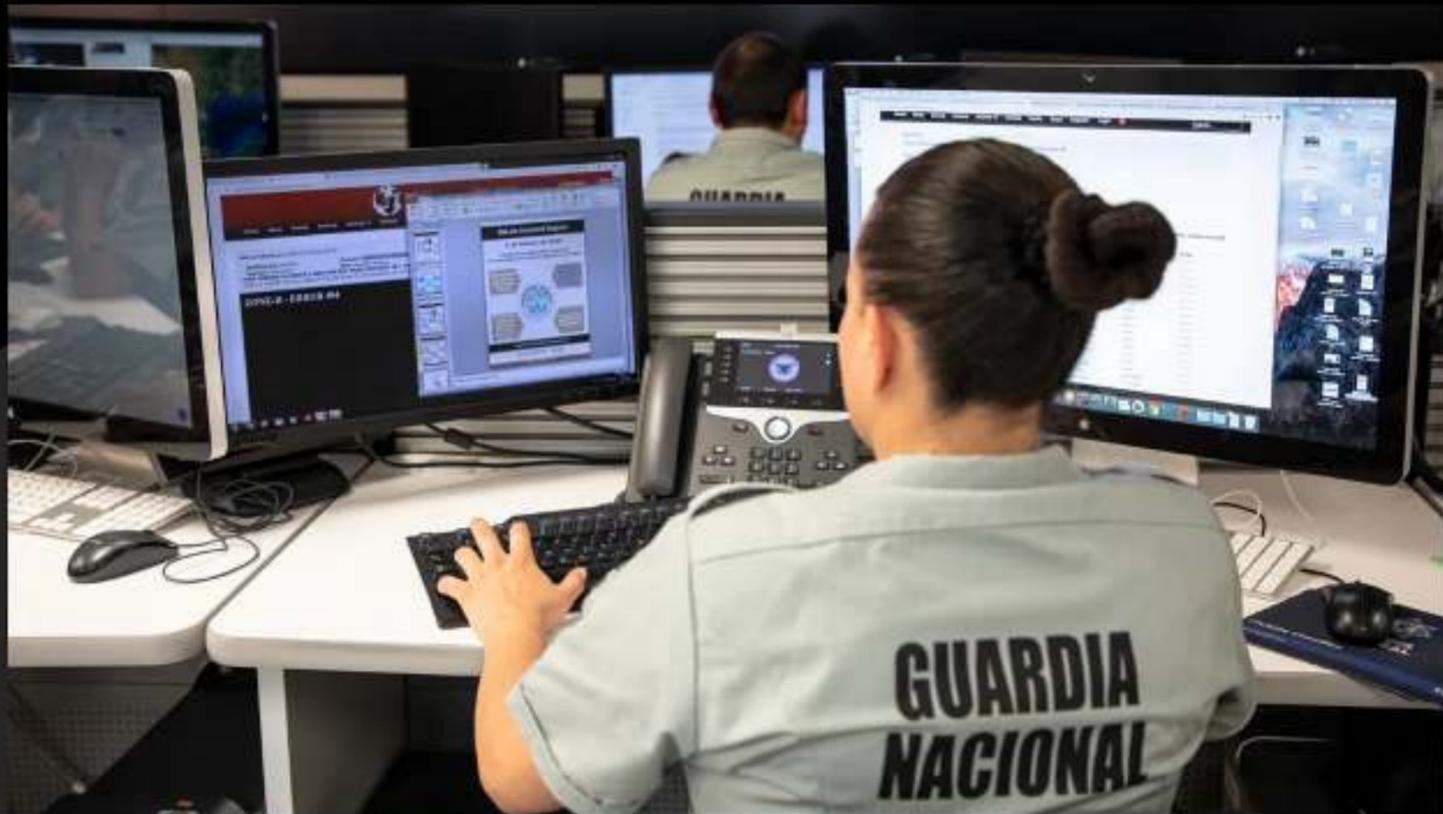
Sistema hegemónico capitalista que espia, lucra y manipula
a sus usuarios-mercancias.

En el caso de comunicadorxs y defensorxs el análisis de riesgo de su ciberseguridad pasa por revisar los posibles agentes maliciosos que atacan a usuarios de manera individual pero hay que enfatizar en el riesgo de las grandes empresas de tecnología y el Estado.

¿Quién provee el internet?

¿Qué tan seguro son esos sistemas informáticos?

¿quien y para que sirven esas redes y aplicaciones que usamos para nuestro trabajo y la relación con nuestros posibles atacantes o adversarios sociales.



Propuesta de empleo de ahorros. <input checked="" type="checkbox"/> Medidas Salariales. <input checked="" type="checkbox"/> Gasto de Op. y Manto. <input checked="" type="checkbox"/> Otras presiones de gasto.	1	Indemnización a personal civil por probables violaciones a los Derechos Humanos.	15.00
	2	Aportación de 20,000 USD anuales para atención de la Junta Interamericana de Defensa. <i>(A un tipo de cambio de \$18.40, equivale a 0.37 MDP.)</i>	0.37
	3	Necesidades del Sistema Educativo Militar "2019".	106.23
Resumen General.	4	Servicio de monitoreo remoto de información. <i>(9'280,000.00 USD. a un tipo de cambio de \$18.40 equivale a \$170'752,000.00 M.N.)</i>	170.75
	5	Construcción de un CEN.D.I. en la 11/a. Bgda. Pol. Mil. (San Pedro de las Colonias, Coah.)	49.02

TODO LO QUE **GOOGLE** SABE SOBRE TI...



CHROME

HISTORIAL DE WEBS
QUE HAS VISITADO.



CALENDAR

EVENTOS A LOS QUE
VAS A ASISTIR.



GMAIL

EMAILS QUE HAS
ENVIADO Y RECIBIDO.



SEARCH

BÚSQUEDAS QUE
HAS REALIZADO.



HANGOUTS

CONVERSACIONES
QUE HAS TENIDO.



MAPS

SITIOS EN LOS QUE
HAS ESTADO.



YOUTUBE

VÍDEOS QUE
HAS VISTO.



PHOTOS

DÓNDE Y CON QUIÉN
TE HAS HECHO FOTOS.



ADS

ANUNCIOS QUE TE
HAN INTERESADO.



DRIVE

DOCUMENTOS QUE
HAS ALMACENADO.



SHOPPING

PRODUCTOS QUE
HAS BUSCADO.



NEWS

NOTICIAS QUE
HAS LEÍDO.

3. Analisis de riesgo y medidas preventivas

modelo TCP / IP

Componentes

Vulnerabilidades

Cuidados

APLICACIÓN

Big Tech
Software
información

Contrato de privacidad
Interceptación de comunicación
Llave de encriptación del
proveedor
Puertas traseras en el software

Uso de Software Libre
Proveedores de confianza
Constraseñas seguras
Actualizaciones

TRANSPORTE

Encapsulamiento
Servidores DNS
Otros ISP

Es conocido el origen y destino
Interceptación de comunicación
Ataques fuerza bruta y otros
suplantación y redireccionamiento

Uso de VPN
Uso de https
Encriptación

CAPA DE RED

Direccionamiento IP
Proveedor Internet (ISP)
Enrutador

Acceso a comunicaciones
Acceso a datos personales

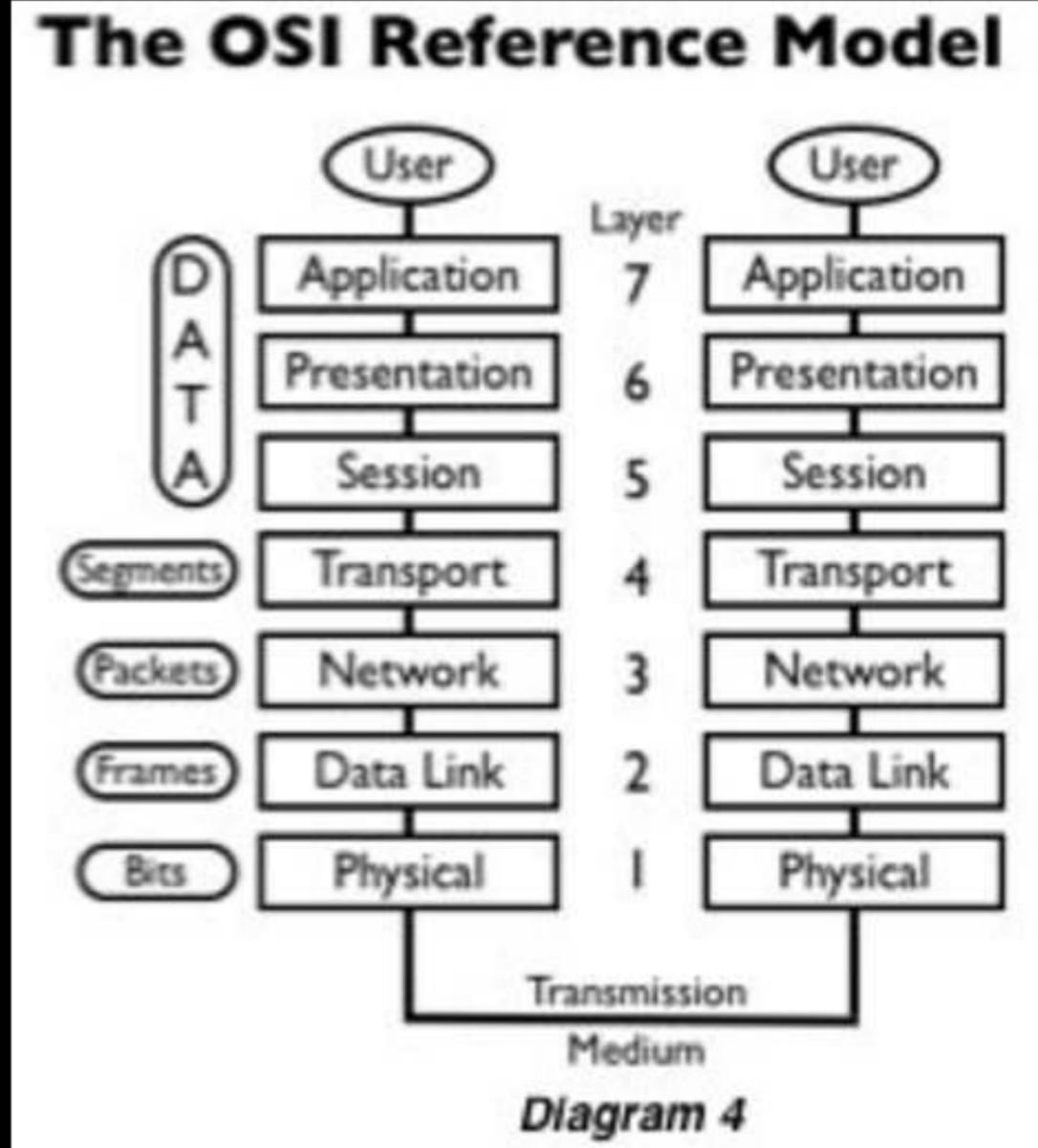
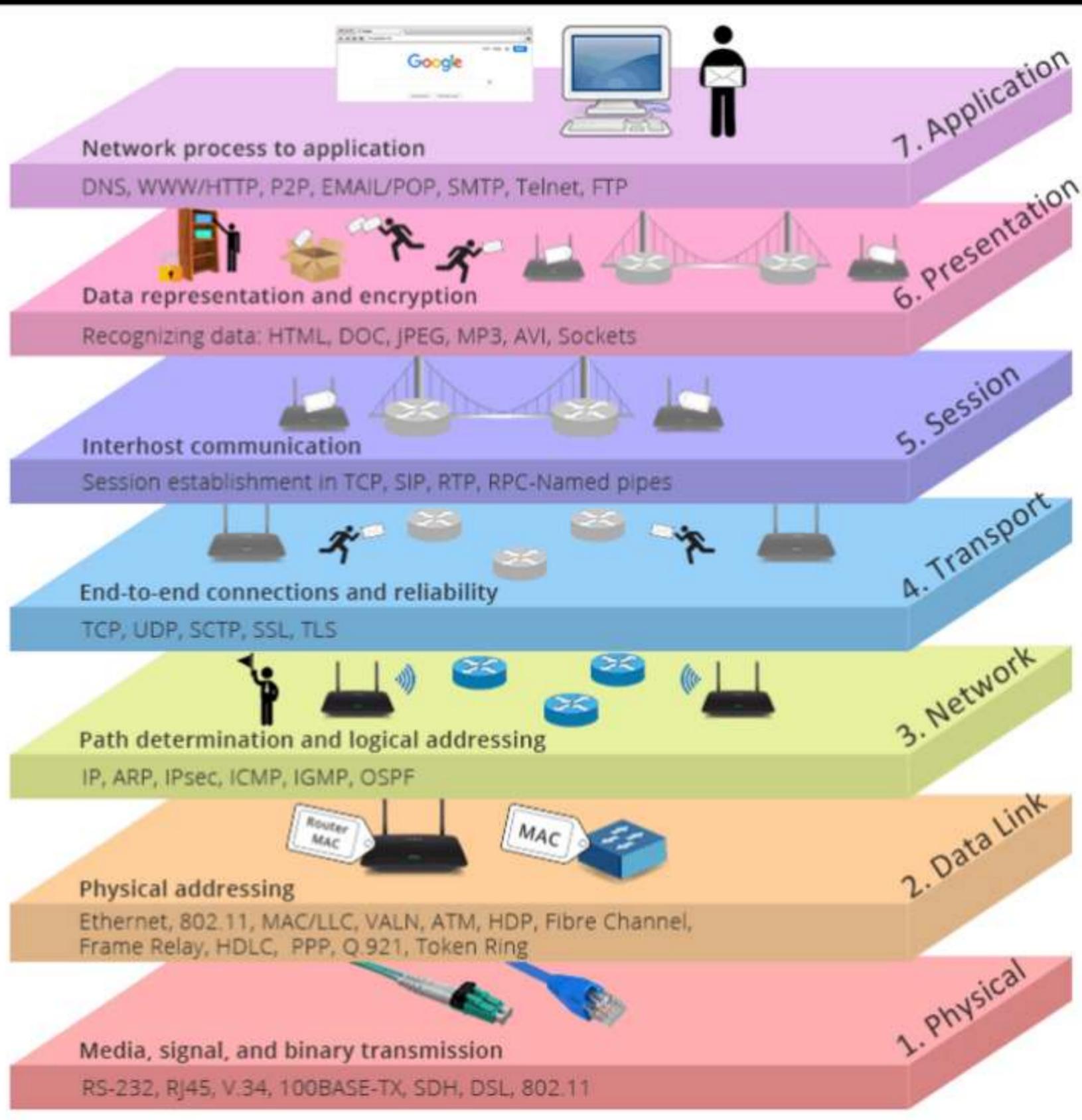
Firewall local
Cambio contraseñas
router
Cambio proveedor

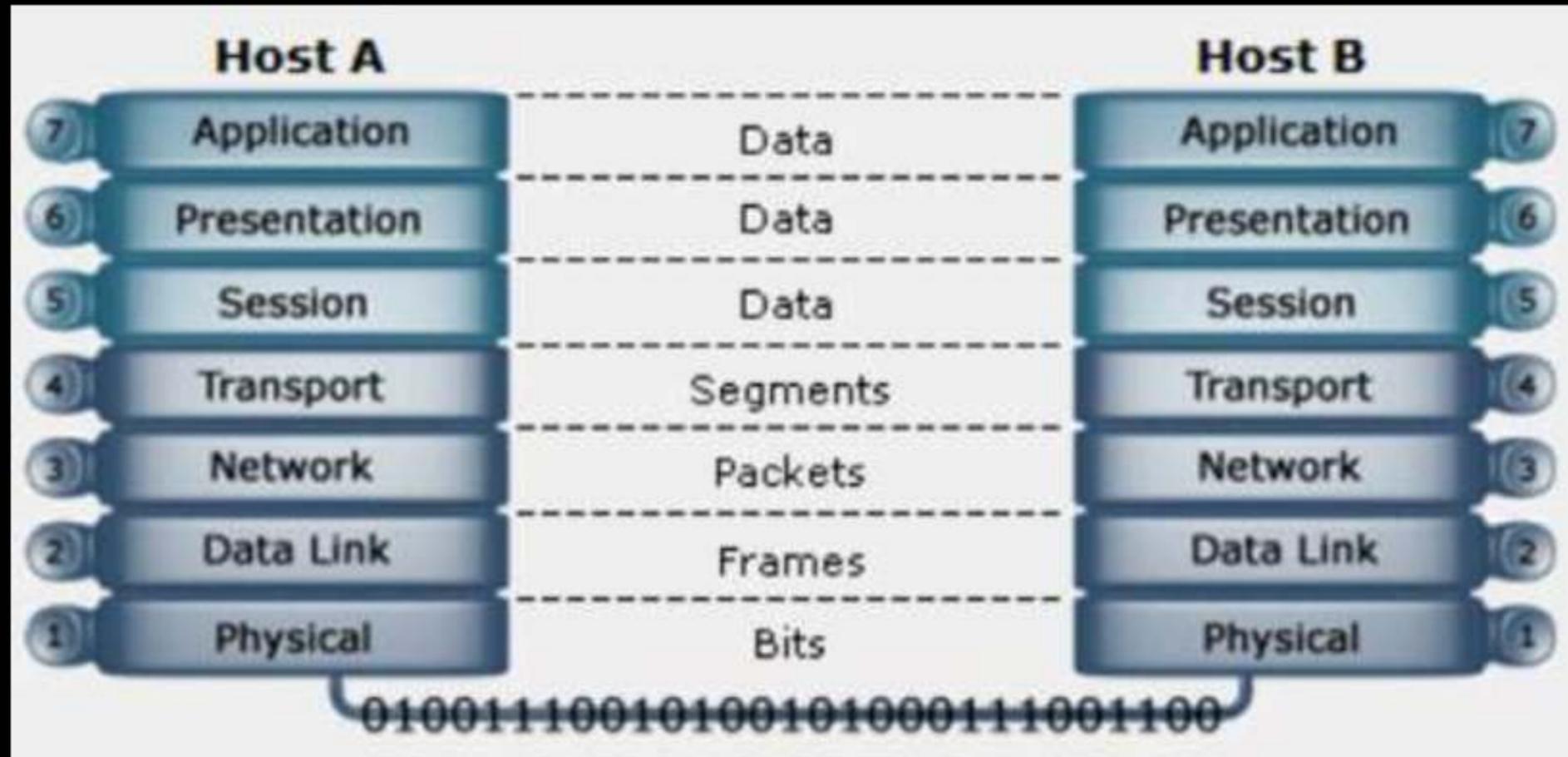
CAPA FÍSICA

Radiofrecuencia - WiFi
Cables de Red
PC, Laptop, celulares, etc

Accesos públicos
intermediario / escuchas
penetración física
robos

Usar conexiones de
confianza
Chekeos periódicos
visuales físicos





Modelo TCP/IP

Capa de aplicación

Capa de transporte

Capa de red

Capa de acceso de red

Familia de protocolo TCP/IP

H
T
T
P

S
M
T
P

T
e
l
e
n
e
t

F
T
P

D
N
S

R
I
P

S
N
M
P

TCP

UDP

ARP

IP

IGMP

ICMP

Ethernet

Token
Ring

ATM

Frame
Relay

¿Como cuidarnos?

SOFTWARE LIBRE OPEN SOURCE

Es un movimiento social para que los usuarios se beneficien libremente con el **uso del software**.

Es una metodología de **desarrollo** para que los programadores se beneficien **al compartir el código**.

4 LIBERTADES

-  **Ejecución libre.**
-  **Estudiar y adaptar** el código fuente.
-  **Distribuir copias.**
-  **Mejorar y hacer público** el software.

-  El código fuente **se puede compartir y distribuir**.
-  Es posible **realizar modificaciones** al código fuente.
-  Permite que los programadores **se beneficien del trabajo de otros**.



- ✓ **Todo Software Libre es Open Source** pero no necesariamente al revés.
- ✓ **Ninguno de los dos** se basa en la gratuidad del software.



osl.ugr.es/catalogo-software-libre-2

<https://www.cdlibre.org/consultar/catalogo/>

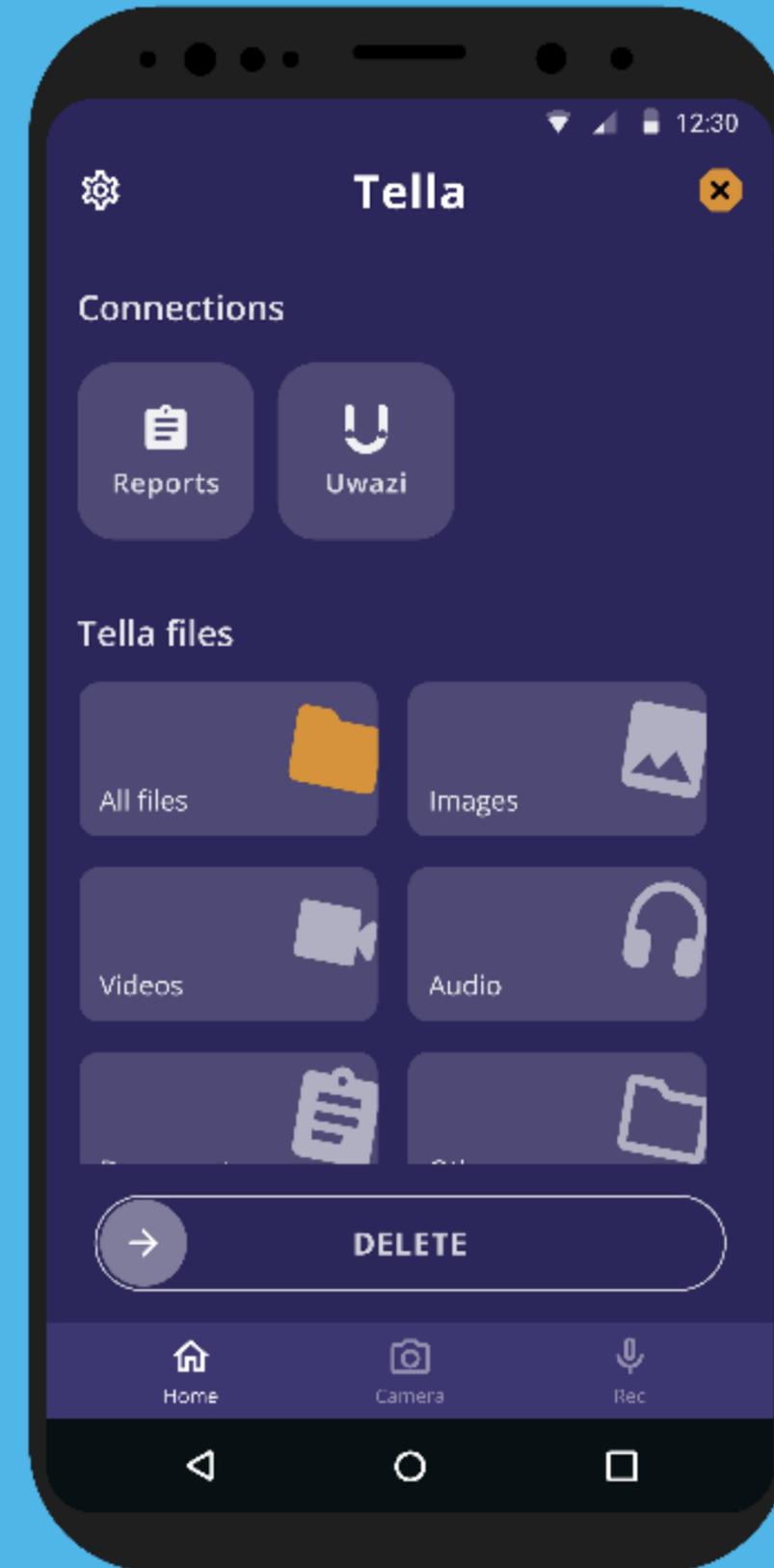
6 Cuidados básicos mínimos para reducir los riesgos y generar protocolos de seguridad personales y colectivos

- 1 Tener contraseñas únicas y fuertes.**
- 2. Busca comunicaciones por canales encriptados.**
- 3. Autenticación multifactor**
- 4. Actualización constante de equipos y aplicaciones.**
- 5. Capacitación y auto aprendizaje**
- 6. Evaluación de los riesgos y Protocolos de seguridad**
- 7. Usar Software Libre (Linux)**

Tella

<https://tella-app.org>

- bloqueo de app
- cifrado de segundo plano
- respaldo en nube
- configurar tiempo de espera
- modo silencioso
- seguridad de pantalla
- restringir intentos de bloqueo
- editar medios
- cifrado
- admin de archivos cifrados
- importar archivos
- analíticas
- camuflaje
- personalización de pantalla de inicio
- audio
- foto y video
- modo verificación
- conexiones en línea
- conexiones fuera de línea



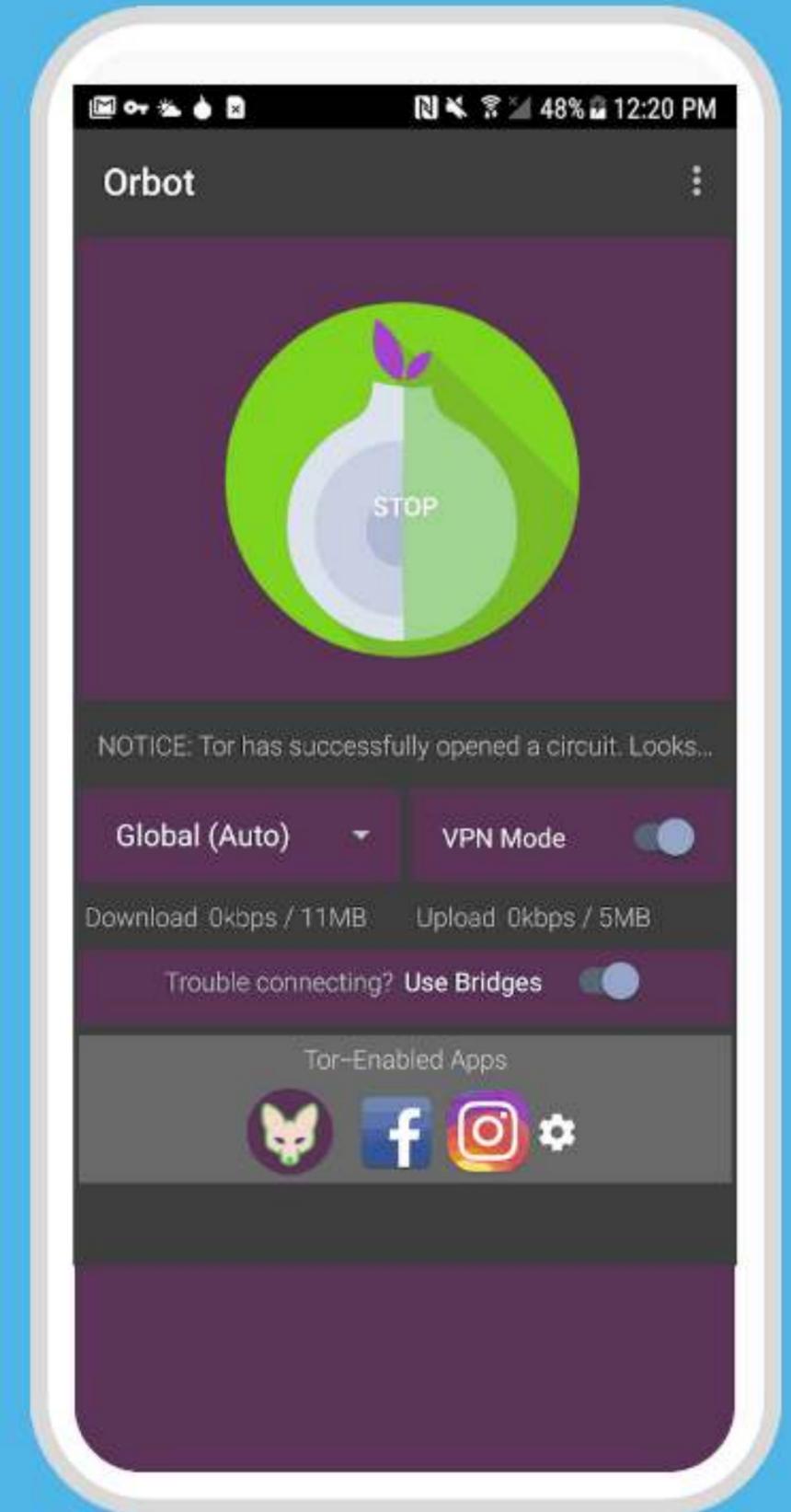
<https://orbot.app/es/>

Tráfico encriptado desde cualquier aplicación, a través de la red Tor, te brinda el más alto nivel de seguridad y privacidad.

Ningún ojo adicional sabe qué aplicaciones estás usando y cuándo, y no te pueden impedir que las uses.

No hay un registro central de tu historial de tráfico o dirección IP por parte de tu operador de red y servidores de aplicaciones.

Orbot (en Android) te permite elegir específicamente qué aplicaciones enrutar a través de Tor, lo que te permite seguir usando aplicaciones y servicios que pueden estar relacionados con el tráfico proveniente de Tor. Orbot ofrece acceso a una variedad de Puentes de Tor, para que puedas mantenerse conectado incluso en las redes más restringidas



Privacy Badger es una extensión de navegador gratuita para Google Chrome, Mozilla Firefox y Opera creada por la Electronic Frontier Foundation (EFF).

Su propósito es promover una aproximación equilibrada a la privacidad en internet entre consumidores y proveedores de contenido bloqueando anuncios y cookies rastreadoras que no respetan las configuraciones de No Seguimiento del usuario
<https://privacybadger.org>



¡La privacidad es un deporte de equipo!

4 tipos de riesgos

TIPO DE RIESGO 1: Malwares

Virus (se adhieren a soft)

Gusanos (tienen vida propia)

Adware (inocuos o malignos)

Troyano (parece otra cosa)

Spyware (espia o roba datos)

Keylogger (guarda claves o tecleo)

Ransomware (secuestra datos wanacry)

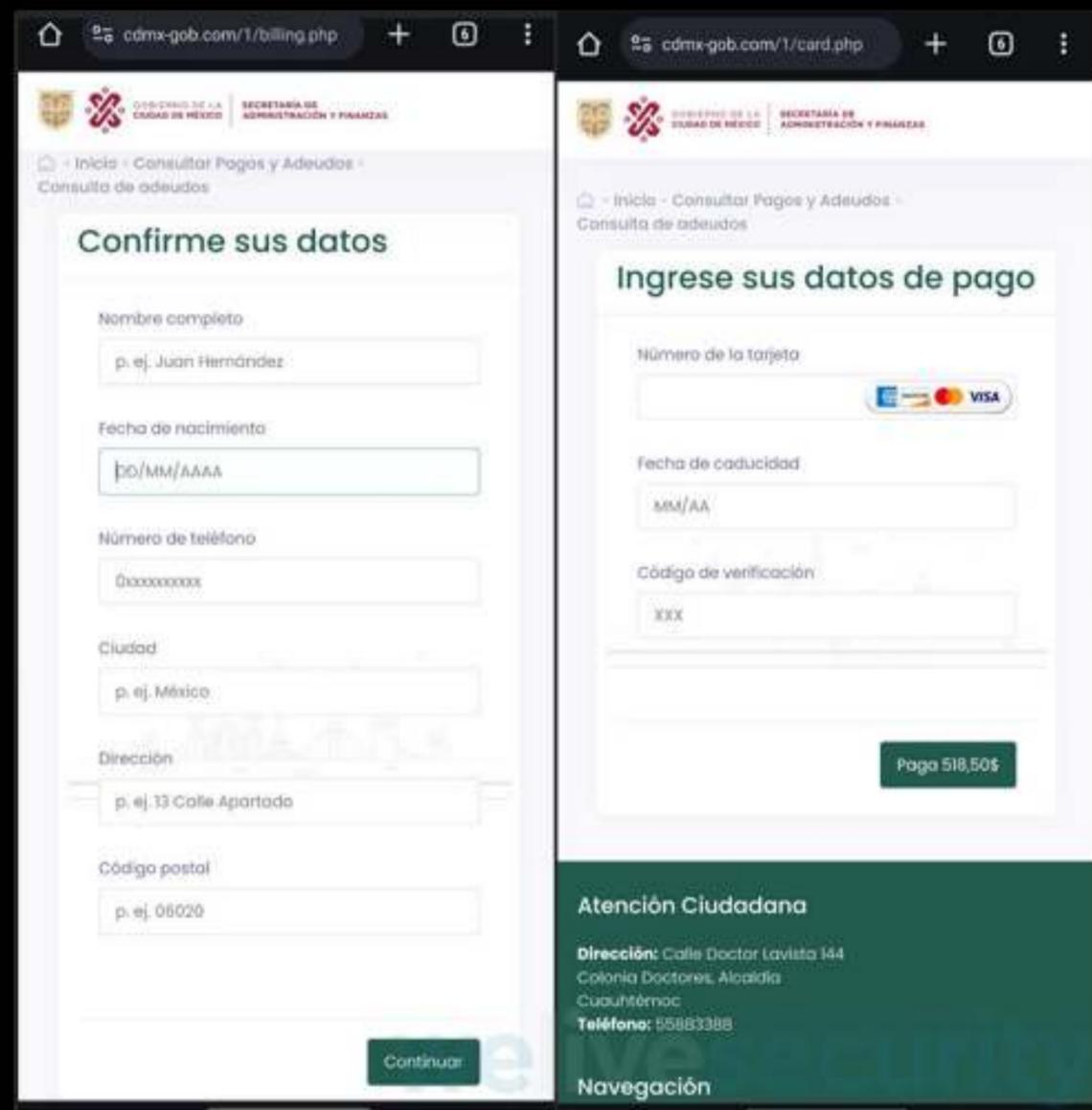
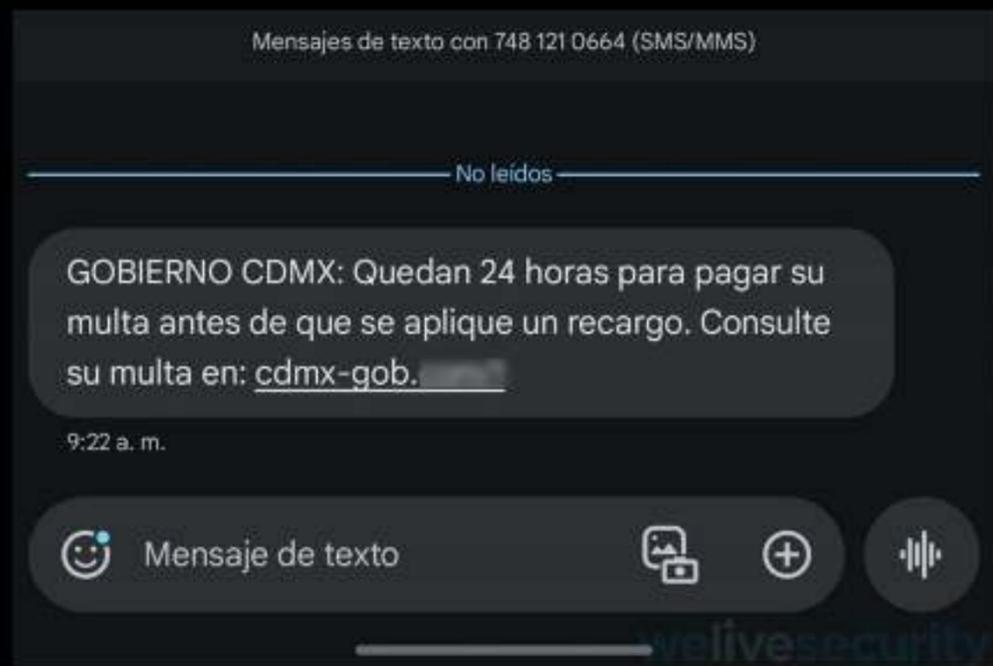
Bots netbots (ocupan tu máquina ram,
kernel, disco duro, etc)

¡Aguas con el phishing y la ingeniería social!

Si dudas de un enlace o documento, primero revísalo

Página para revisar archivos y enlaces dudosos

<https://www.virustotal.com/>



Ayer • 15:08

Santander banco : Lo invitamos a confirmar rapidamente su informacion para evitar una resticcion o suspension du su cuenta. Haga clic aqui <https://is.gd/AfOXBs>

lun., 15:08

Mensaje de texto

lunes, Hoy

Nuestro sistema nos alerta de un pre-cargo no autorizado de 398,99 EUR con su tarjeta. Para cancelar el pago sigue nuestro enlace: <https://t.ly/cancelar>

Hace 26 min.

← +52 221 243 5541

BLOCK | ADD

15 July 2021

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

¿Hola, necesitas un trabajo a tiempo parcial? Salario mensual 💰 *9000 - 15000 *,
MXN * 300 * al menos todos los días.
No hay cargo por servicio.
El trabajo simple se puede hacer en casa.
Si está interesado en este trabajo, póngase en contacto con WhatsApp: <http://wa.me/6283815015992>
Por favor, responda * 1 * activar enlace

5:04 pm

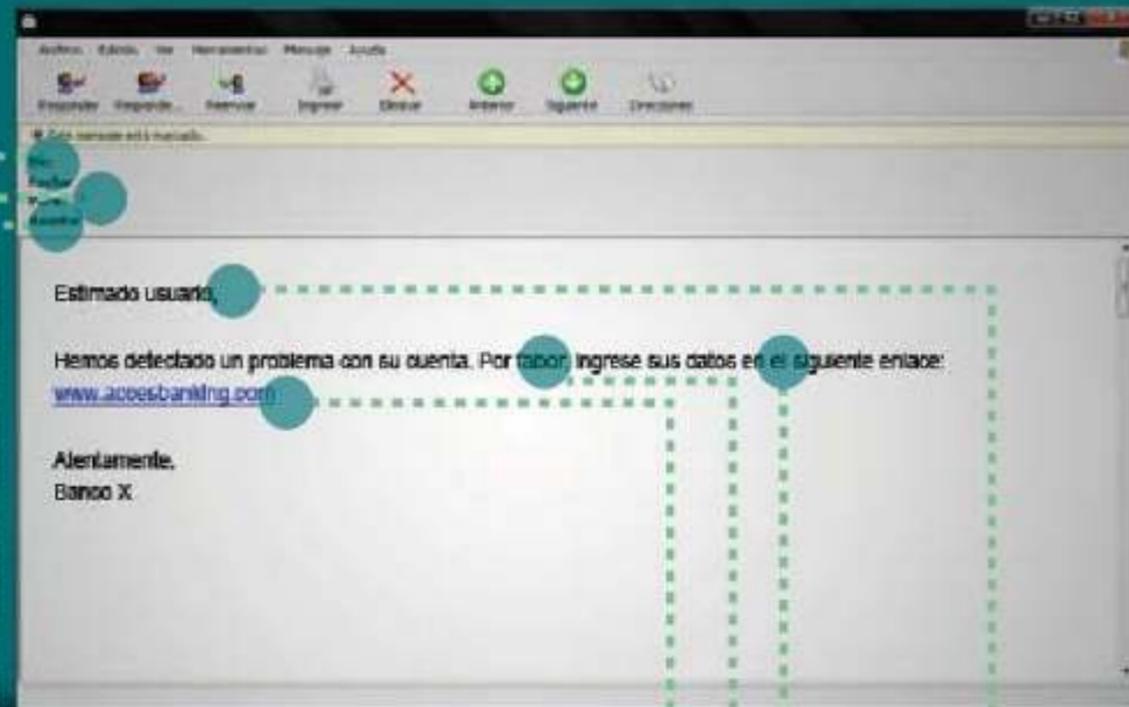
Ayer • 15:08

Santander banco : Lo invitamos a confirmar rapidamente su informacion para evitar una resticcion o suspension du su cuenta. Haga clic aqui <https://is.gd/AfOXBs>

lun., 15:08

E-mail

Los correos electrónicos buscan llamar la atención del usuario con mensajes de alerta aunque en general no están dirigidos de manera personal.

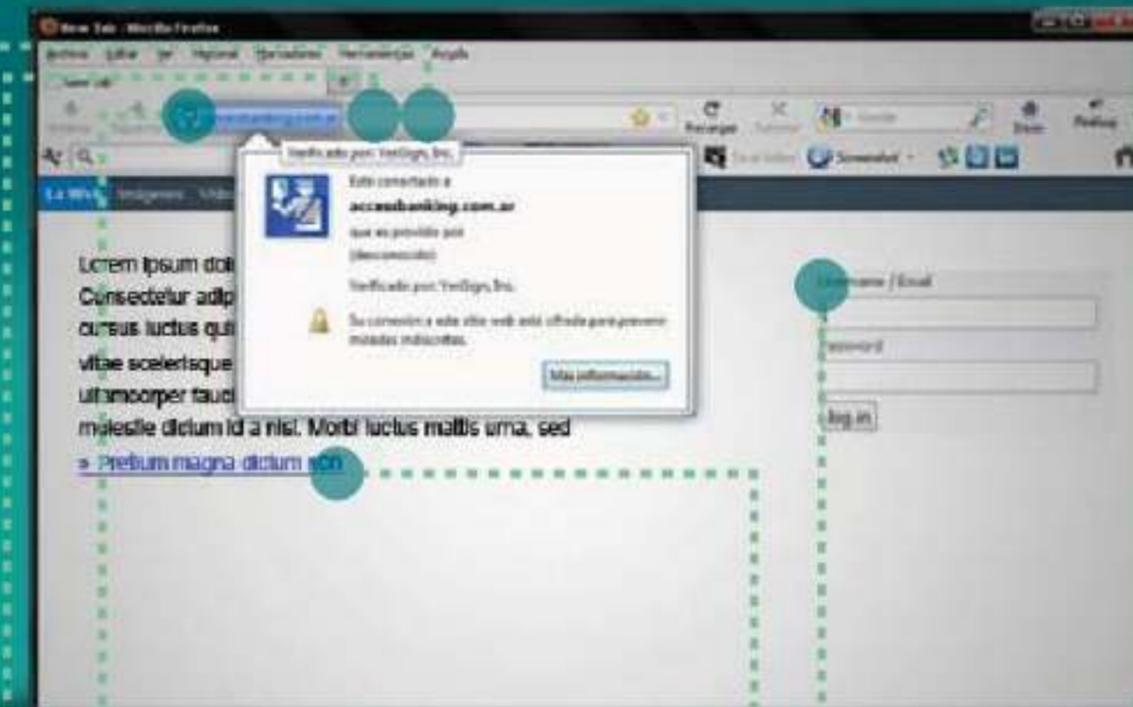


- De:** Mensajes de remitentes desconocidos.
- Para:** Mensajes con muchos destinatarios y desconocidos.
- Asunto:** Asunto del mensaje trata temas inusuales para el usuario.
- A veces el link del cuerpo del correo no coincide con el que se puede ver en la barra de estado del navegador.

- Se dirige a un usuario genérico: "Estimado usuario/cliente/etc."
- Mensaje de alerta con un llamado a la acción.
- Errores de ortografía.

Sitio web

La web puede ser muy similar pero en muchos casos no es exactamente la misma que la legítima, y al chequear la URL o su seguridad debería haber diferencias.



- Identificar el candado de certificado de seguridad.
- Verificar que el certificado de seguridad coincida con la URL a la que se está accediendo.
- http** Comprobar el protocolo seguro: https.
- www** Verificar URL.

- Pide datos de acceso fuera de lo normal.
- Cuando haya enlaces acortados, poner el mouse encima para verificar la dirección de destino.

¿QUÉ TIPO DE INFORMACIÓN ROBA?

PRINCIPALES MEDIOS DE PROPAGACIÓN

Direcciones de correo



Datos personales



Número de documento de identidad



Datos de localización y contacto



Número de tarjetas de crédito



Información financiera



Números de cuentas



Información de Home Banking o e-commerce



Credenciales de acceso



Redes Sociales



Cuentas de correo



Correo electrónico



Redes Sociales



SMS/MMS



Llamados telefónicos



Infección de malware

Análisis de amenazas y protocolo de seguridad

¿De dónde o quién vienen estas amenazas?

¿Cuál es la capacidad del atacante?

¿Qué tan probable es que ocurra?

¿Cuál será el impacto?

¿Cómo se puede mitigar esas vulnerabilidades?

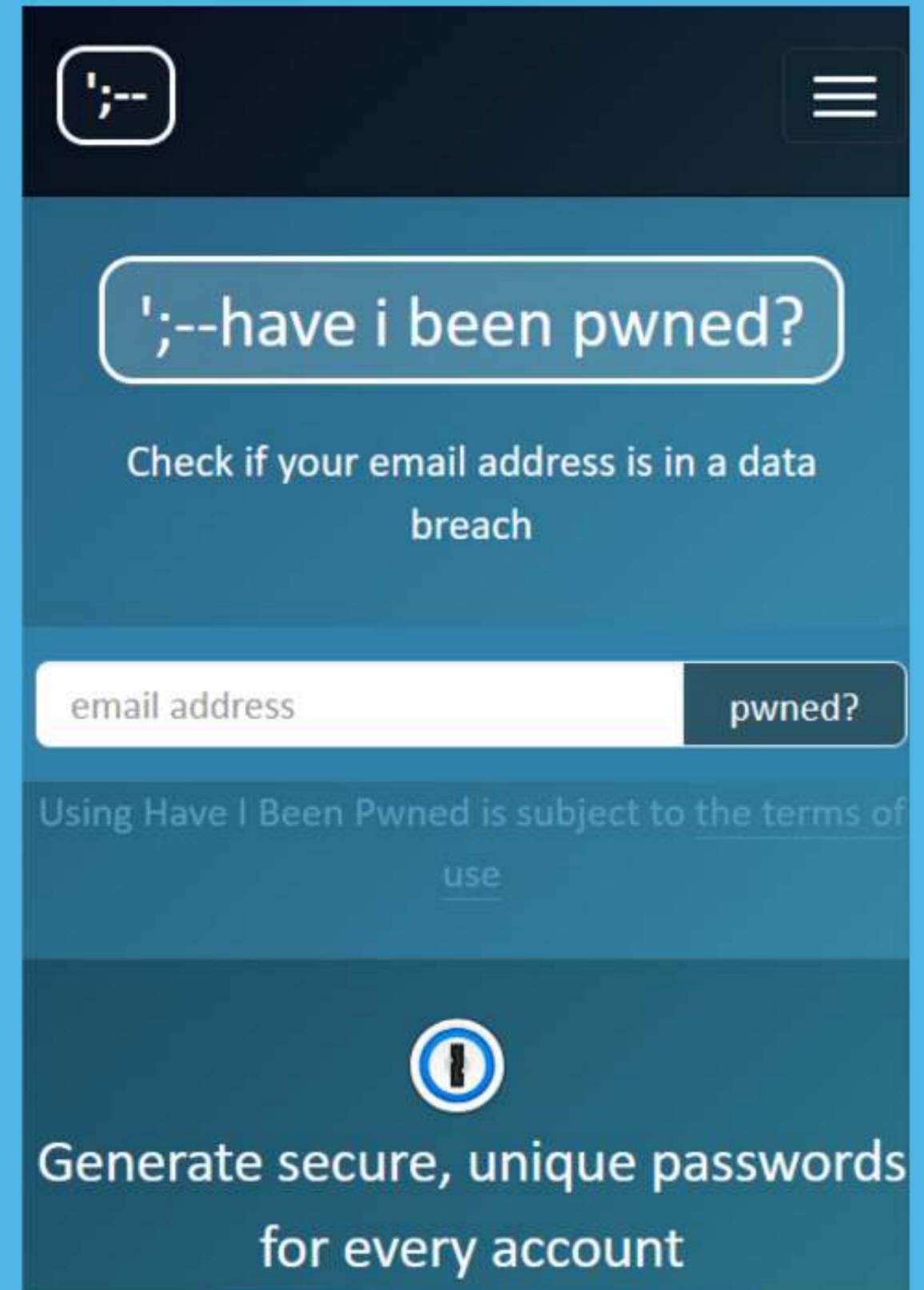
¿Cómo prevenir, resolver y recuperar de un posible ataque?

https://haveibeenpwned.com/

Es un sitio web que permite a los usuarios de Internet comprobar si sus datos personales se han visto comprometidos por violaciones de datos.

El servicio recopila y analiza cientos de ficheros de bases de datos que contienen información sobre miles de millones de cuentas filtradas, y permite a los usuarios buscar su propia información introduciendo su nombre de usuario o dirección de correo electrónico.

Los usuarios también pueden inscribirse para que se les notifique si su dirección de correo electrónico aparece en futuros volcados

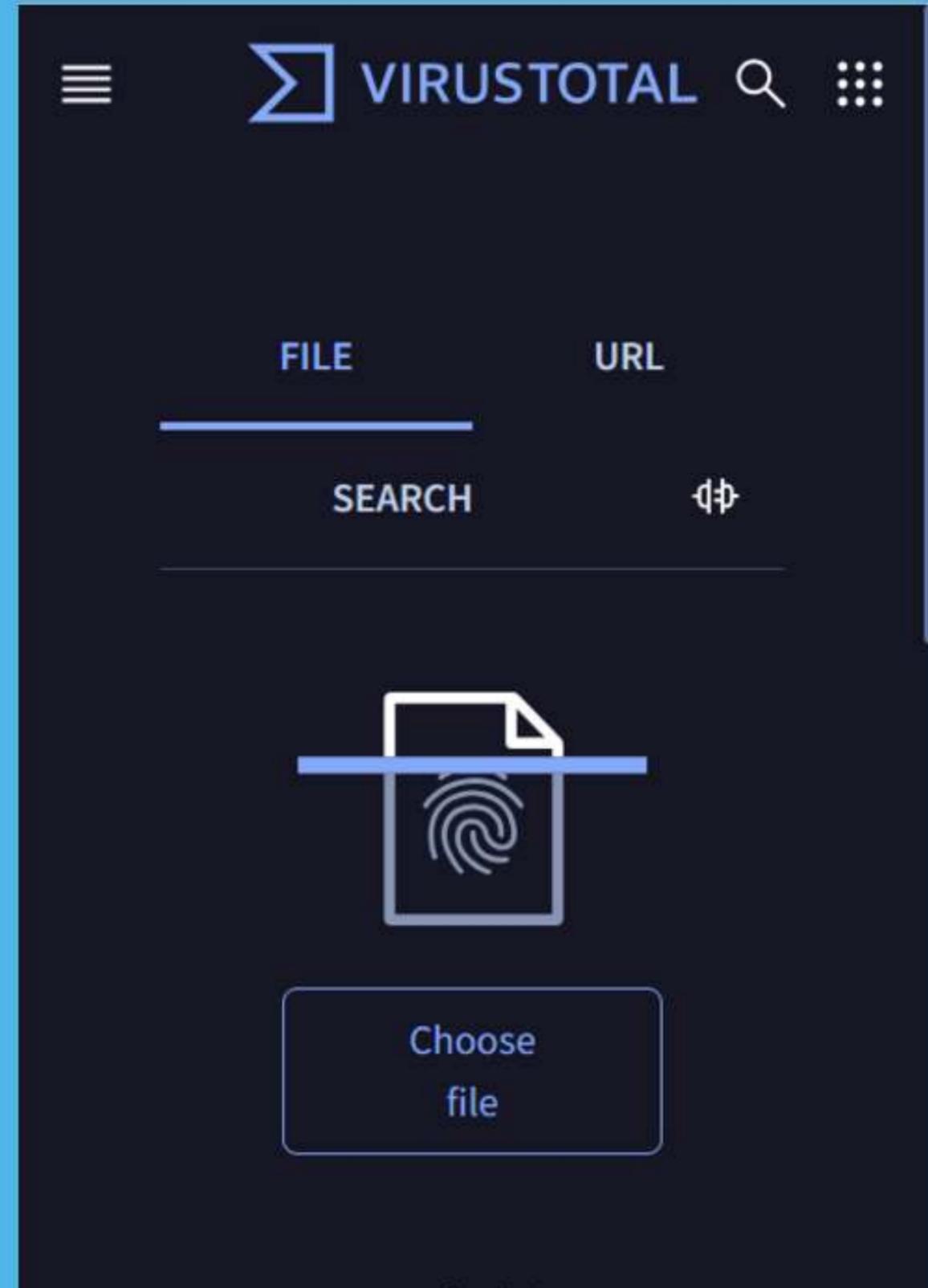


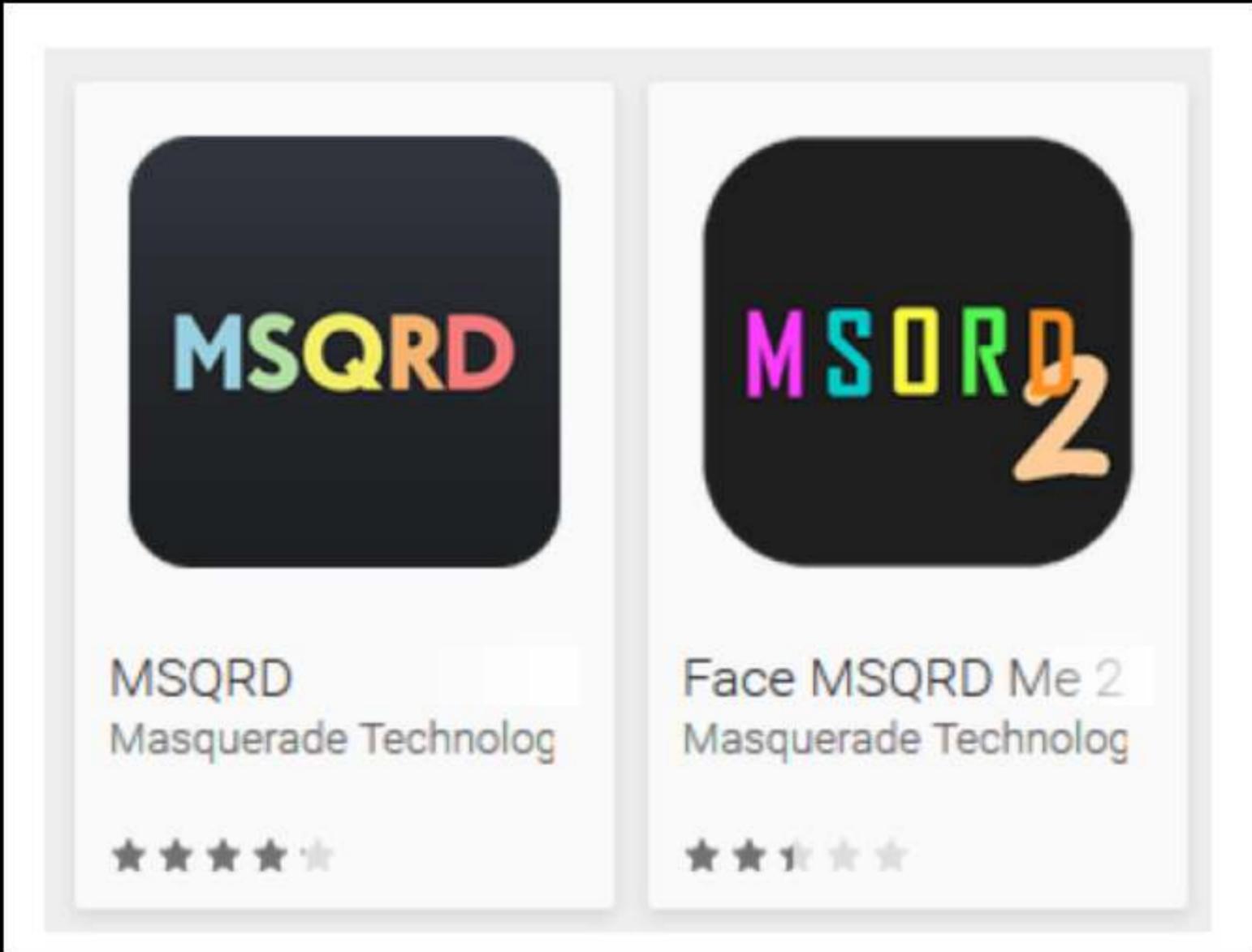
The screenshot shows the homepage of the website. At the top left is a logo with the text 'have i been pwned?' and a search icon. At the top right is a hamburger menu icon. Below the logo is a large search input field containing the text 'have i been pwned?'. Underneath the search field is the text 'Check if your email address is in a data breach'. Below that is a search input field with the placeholder text 'email address' and a button labeled 'pwned?'. At the bottom of the page is a blue banner with a padlock icon and the text 'Generate secure, unique passwords for every account'. A small link for 'terms of use' is visible in the footer area.

www.virustotal.com

VirusTotal es una herramienta en línea que analiza archivos, URL, direcciones IP y dominios sospechosos para detectar software malicioso y otros tipos de amenazas:

- Utiliza más de 90 antivirus en línea
- Proporciona un informe con los resultados del análisis
- Comprende si el archivo o recurso web ha sido marcado como confiable en todos los análisis
- Ofrece información sobre el motivo por el que no se está marcando como confiable





Re-ind
@ReBensk

#Android #PlayStore #Banking #Trojan #Malware
#AndroidSecurity @malwrhunterteam
@cryptax @LukasStefanko
@bl4ckh0l3z @mobilesecurity_
@JAMESWT_MHT @500mk500
@ni_fi_70
#Joker Trojan on Google Play :
[play.google.com/store/apps/det...](https://play.google.com/store/apps/details?id=Md5:1325ddc84a95033801f4043f260c8313)
Md5: 1325ddc84a95033801f4043f260c8313
[Traducir Tweet](#)



play.google.com
PDF Reader Scanner - Apps on Google Play
A PDF reading and scanning tool.

1:59 a. m. · 26 jun. 2022 · Twitter Web App

Webcam

- Cover cameras when not in use.



Web Browser

- Ensure transit security encryption, usually with a lock icon in the address bar.



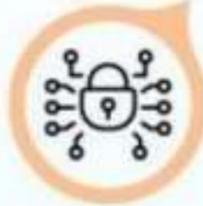
External Storage

- Back up data on external drives or portable media.



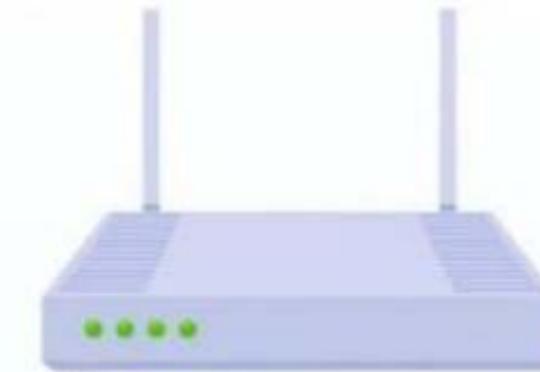
Home Assistance

- Limit nearby sensitive conversations.
- Mute microphones when not in use.



Laptop/Computer

- Utilize a non-privileged "user" account for everyday activities.
- Update with the latest patches, preferably through automatic updates.



Wireless Access Point/Router

- Use WPA3 or WPA2/3 with protected management frames.
- Update with the latest patches, preferably through automatic updates.
- Schedule weekly reboots.



Figure: Several best practices for securing your home network

Laboratorio Popular de Medios Libres

<https://laboratoriomedios.org/>

contacto@yanapak.org

ORGANIZE
EDUCATE
RESIST



**Bienvenidos al curso de introducción
a Seguridad Informática.**



**¡Ya Hackea el sitio de una vez,
maldita sea!**