

Securización del entorno de trabajo



Contenidos

1. Introducción.
 1. Identificación de usuarios.
 2. Contramedidas.
2. Estado de privacidad de los equipos.
 1. Análisis de huellas digitales.
 2. Herramientas de anonimización.
3. Generación de identidades falsas.

Introducción

- ▶ La navegación a través de Internet y el uso de herramientas digitales genera **huellas**.
- ▶ Estas huellas son únicas, por lo que **pueden identificar unívocamente a un usuario**.
- ▶ Ejemplo: www.balizasdigitales.es



Introducción

► Contramedidas.

- Evitar la geolocalización de los mensajes en las redes sociales, imágenes, dispositivos móviles...
- No abrir emails de remitentes desconocidos (podrían obtener nuestra IP según la configuración del navegador).
- Utilizar siempre 2FA o dispositivos hardware.
- Revisar permisos de apps móviles y software del PC. (Ej: [CONAN Mobile](#))

Introducción

► Contramedidas.

- Desconfiar de solicitudes de amistad o seguimiento en redes sociales por parte de desconocidos/as.
- Separar la vida personal y profesional. Ideal: equipos diferentes. Si no es posible, entornos aislados con máquinas virtuales.
- ***Egosurfing***. Usar alertas de Google (dni, pasaporte, teléfono, dirección...).

Estado de privacidad de los equipos

- ▶ **Análisis de huellas digitales.**
 - **Cover Your Tracks**. Proyecto de la EFF (*Electronic Frontier Foundation*). Verifica las huellas que deja el navegador.
 - La EFF recomienda instalar la extensión **Privacy Badger** (no bloquea anuncios, solo rastreadores).
 - Mayor protección: Tor Browser, Brave...
 - **Trackography**. Muestra con quién comparte información diferentes web de noticias.

Estado de privacidad de los equipos

► Herramientas para la anonimización.

– **Prism-Break.** <https://prism-break.org/es/>









- PRISM es un programa secreto de vigilancia mundial organizado por la NSA y hecho público por Eduard Snowden.
- *Prism-break* es un proyecto que recopila herramientas y tecnologías para salir de esos proyectos de vigilancia.

PRISM ⚡ BREAK

Todos los Proyectos Plataformas Protocolos Acerca de Dona Bitcoin

Opta por salir de los programas globales de vigilancia de datos como [PRISM](#), [XKeyscore](#) y [Tempora](#).

Impide que los gobiernos te espíen cifrando tus comunicaciones y terminando tu dependencia en servicios privativos.

Móvil	 Android	>
	 iOS	>
Ordenador	 BSD	>
	 GNU/Linux	>
	 macOS	>
	 Windows	>
Red	 Routers	>
	 Servidores	>

Estado de privacidad de los equipos

► Herramientas para la anonimización.

– **Privacy Tools.** <https://www.privacytools.io/>

- Web que recopila multitud de herramientas y consejos para configurarlas, maximizar la privacidad y evitar el seguimiento.



Estado de privacidad de los equipos

► Herramientas para la anonimización.

- **4nonimizer**. <https://github.com/Hackplayers/4nonimizer>
 - Es un script en bash para ocultar la IP pública empleando conexiones con Tor y diferentes VPNs.
 - Creado por Carlos Antonini y Vicente Motos ([Hackplayers](#))



Estado de privacidad de los equipos

► Herramientas para la anonimización.

- **Modo incógnito.** No guarda información pero no proporciona anonimato.
- **VPN.** Oculta nuestra IP de origen. ([10 mejores VPN 2021](#))
 - [F-Secure Freedom](#). VPN de pago (unos 5€/mes para 5 dispositivos).
 - [UltraSurf](#). Herramienta libre, disponible para Windows y Android, que permite saltarse restricciones y censura (muy utilizado en estados totalitarios).
 - [Windscribe](#). Ofrece privacidad para limitar el trackeo y seguimiento de las web. Disponible para todos los sistemas operativos, navegadores web y móviles. Acceso libre y de pago.
 - **Navegadores.** [Opera](#), [Mozilla Firefox](#) y otros disponen de herramientas VPN. El navegador [Brave](#) también ofrece conexiones privadas y VPNs.
- **TOR y similares.** Algunas páginas que nos pueden interesar bloquean el acceso si detectan que la conexión proviene de este tipo de redepros.
- **ORBOT.** Similar a Tor para el teléfono.
- **Distribución Tails** (*The amnesic incognito live system*). Uso de un pendrive de arranque.
- Confeccionar un entorno virtual con las herramientas que necesitamos. Ejemplo para usar de base: [Whonix](#).

Generación de identidades falsas

- ▶ Necesitamos identidades falsas para que nos ayuden a nuestras investigaciones.
- ▶ Herramientas para generar nombres falsos:
 - Fakenamgenerator.
<https://www.fakenamgenerator.com/>
 - Namefake.com. <https://en.namefake.com/>
- ▶ Buzones de correo electrónico temporal:
 - <https://correotemporal.org/>
 - Guerrillamail.com (recibir y enviar).
 - <https://temp-mail.org/>

Generación de identidades falsas

► Generación de Imágenes.

- <https://thispersondoesnotexist.com/>
- <https://generated.photos/>
- Faceapp. <https://www.faceapp.com/>
- <https://www.whichfaceisreal.com/>

► Imágenes mediante Inteligencia Artificial.

- Stable Diffusion.
- Craiyon.
- Buscador [Lexica.art](https://www.lexica.art/).

FIN