femh^(k

encuentro/taller *hackear* nuestras prácticas: género y tecnología

san cristóbal de las casas
mayo, 2015

respaldos

El consejo más importante que podemos ofrecer a cualquier organización, colectivo o individuo es **siempre mantener respaldos** de su información digital más importante.

De nada te servirán técnicas más avanzadas de seguridad si pierdes tu información por una falla mecánica o eléctrica

¿**dónde**?

discos duros

discos ópticos

blu-ray

memorias usb

la nube

aspecto físico

Evita compartir tu computadora o dispositivos con desconocidos

Evita utilizar conexiones a wifi públicas (y si necesitas hacerlo toma algunas medidas)

Evita compartir tus discos duros o memorias usb

Evita descuidar tus equipos, bah...

contraseñas seguras

Tips:

(1) No datos asociados a ti misma
(2) No repetir
(3) No las compartas
(4) No la anotes en un *post it*
(5) Cámbiala periódicamente
(6) ¡Utiliza todo tipo de caracteres!

¿y cómo las recuerdo todas?

gestor de contraseñas keepass (herramienta de administración de contraseñas FOSS segura y fácil de utilizar)

http://www.keepass.info/

borrado de metadata

Tips:

(1) Metadatas son todos aquellos datos que se guardan “por fuera de nuestros archivos”
(2) Brindan gran cantidad de información sobre nosotras
(3) Antes de enviar un archivo, ¡no dejes rastros!

Exiftool para Win, Mac y Linux (solo por consola)
http://owl.phy.queensu.ca/~phil/exiftool/

MAT (modo gráfico) para Linux https://mat.boum.org/

borrado seguro de datos

Tips:

(1) No conserves archivos que no te sirvan
(2) Borrar no destruye la información solo elimina el punto de anclaje
(3) Elimina espacio no usado y metadatos regularmente

una computadora limpia, es una computadora feliz

-Eraser http://www.heidi.ie/eraser/ **y Ccleaner** http://www.ccleaner.com/ **para Win**

-En el Finder >> *Vaciar Papelera de Forma Segura* y en *Utilidad de Disco* para borrar de manera segura un disco completo

-Wipe y BleachBit para Linux

navegar la Red con Firefox

¿Dónde está? https://www.mozilla.org/es-AR/firefox/new/

Tips:

(1) Configúralo para eliminar periódicamente el caché
(2) No dejes almacenadas tus contraseñas allí
(3) No permitas que los sitios te rastreen
(4) Elimina tu historial

además tenemos algunos complementos que nos pueden ayudar!

Hola **desde**
http://hola.org/

HTTPS Everywhere **desde**
https://www.eff.org/https-everywhere

desde 'Complementos'
de Firefox

{

Ghostery
AddBlock Plus
NoScript
Better Privacy

a buscar se ha dicho

Parece que Google "lo tiene todo" pero...

(1) Nos rastrea permanentemente
(2) Administra burbujas de filtros
(3) Somos su producto

hay otras opciones para encontrar lo que buscamos...

Searx: https://searx.laquadrature.net/
DuckDuckGo: https://duckduckgo.com
StartPage: https://startpage.com
Ixquick: https://ixquick.com

y a organizarnos, también

Los pads son herramientas de trabajo colaborativo muy útiles para organizarnos en red

(1) Se autodestruyen si no se utilizan
(2) Remiten a quien hace las colaboraciones
(3) Tienen chat insertado
(4) Pueden ser públicos o privados (con contraseña)

¿cuáles usar?

Riseup: https://pad.riseup.net
Titanpad: https://titanpad.com/
Mozilla: https://etherpad.mozilla.org/

buenas prácticas para proteger tus datos personales

(1) Intenta navegar siempre con páginas web de confianza
(2) No aceptes a desconocidos en las redes sociales
(3) Configura las opciones de privacidad de tus cuentas en redes sociales
(4) Recuerda: lo que publicas no te pertenece
(5) Cierra tus sesiones en Internet
(6) Después de usar el navegador elimina el caché (contenidos que visitaste)
(7) Es útil realizar búsquedas aleatorias
(8) Mantén actualizado tus sistema operativo
(9) Encripta y cuida especialmente los archivos valiosos

7 pasos para la Seguridad Digital

(1) El conocimiento es poder: saber qué tipo de hostigamiento recibes, de quién lo recibes y qué podría hacer esa otra persona con tu información, ¿para qué la querría?
(2) Piensa en el punto débil: “El antiguo adagio "una cadena es tan fuerte como su eslabón más débil" se aplica a la seguridad también: el sistema en su conjunto es tan fuerte como el componente más débil”.
(3) Más simple es más seguro y fácil: cuantos menos dispositivos manejemos, ¡mejor!
(4) Más caro no significa más seguro
(5) Está bien confiar en *Alguien* (pero siempre saber en quién estás confiando)
(6) No hay seguridad perfecta, siempre hay un sacrificio
(7) Lo que es seguro hoy puede no ser seguro mañana

¡La seguridad es un proceso!

somos seres gregarios:
las redes sociales digitales

las redes sociales digitales comerciales pueden ser muy útiles para difundir información pero necesitamos saber usarlas...

(1) Somos el producto
(2) Nos rastrean
(3) También tienen burbujas de filtros
(4) Todo lo que sale a internet ya no nos pertenece

para ver: Protege tus redes sociales:
Revisar Facebook y Twitter

¿hay alternativas?

Diáspora: https://diasporafoundation.org/

GNU/Social: https://gnu.io/social/

¿y si está muy largo?

los acortadores de enlaces pueden llevarnos a lugares peligrosos... sin embargo algunos nos permiten compartir lo que queremos utilizando protocolos de seguridad

Dos de ellos pueden ser

https://links.ssl.com/
https://itsssl.com/

esa *antigüedad* llamada correo electrónico

los correo electrónicos comerciales tienen cada vez más desventajas

(1) Almacenan datos privados de sus usuarios… si te piden datos personales “reales”, mejor ni te registres!
(2) Todos los archivos que adjuntes y la información que envíes puede ser usada por la empresa sin previo aviso
(3) Venden tus datos y colaboran con agencias gubernamentales
(4) Almacenan las IP’s desde donde te conectas… o sea, nos rastrean!
(5) También tienen burbujas de filtros

¿hay alternativas?

Open Mail Box: https://www.openmailbox.org/

Riseup: https://help.riseup.net/

Inventati: http://www.inventati.org/es/index.html

chat encriptado inicial

ya que tenemos Firefox como nuestro navegador favorito

ahora podemos tener CryptoCat

(1) También es compatible con varios navegadores
(2) Se pueden enviar y recibir archivos
(3) Permite crear salas
(4) Permite conectarse desde el chat de Facebook
(5) Crea llaves únicas para cada sesión

¿dónde lo encuentro?

https://crypto.cat/

videollamadas

¡es cada vez más fácil!

https://meet.jit.si/

es posible usar Jitsi directamente desde una pestaña del navegador Chrome/Chromium, sin iniciar sesión y sin instalar nada adicional. Escribes la dirección en la barra del navegador y ya estás dentro. Solo es necesario autorizar el uso de tu micrófono y tu videocámara y listo!

Vigilancia masiva

¿Cómo nos vigilan en la red?

pero si yo *no hago nada...* ¿qué les puede interesar de mi vida?

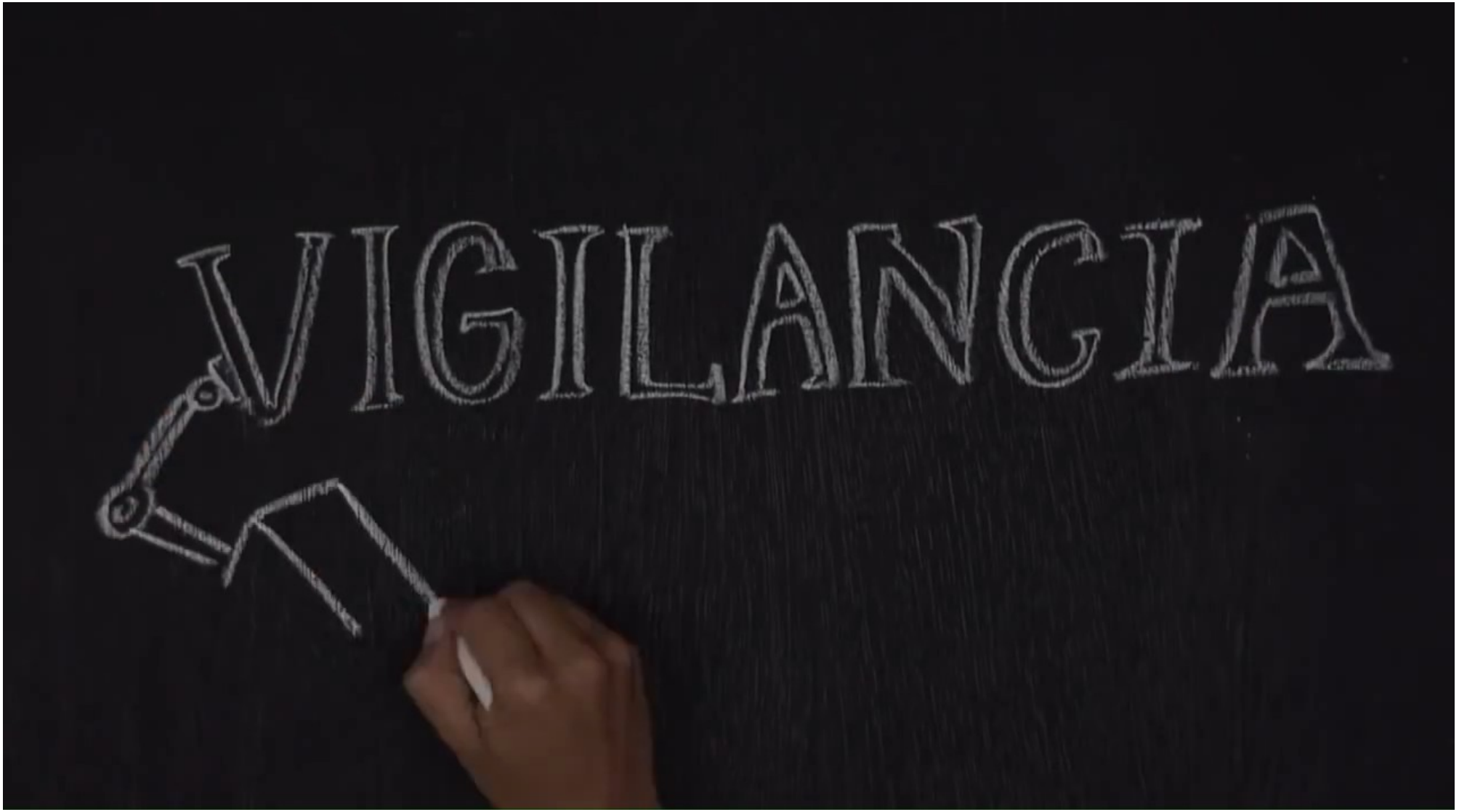
vamos a ver cuántos rastros dejamos en nuestra navegación cotidiana

ingresamos en https://myshadow.org/es/
completamos el formulario
y *¡vualá!*
mira cuántos rastros dejamos

(checa también las recomendaciones que nos dan para estar menos vigiladas...)

vigilancia masiva

https://www.youtube.com/watch?v=tnDxRjMDGQMN



navegación segura con TOR

Ofrece privacidad y anonimato en línea enmascarando quién eres y desde dónde estás conectado. También te protege en la misma red Tor.

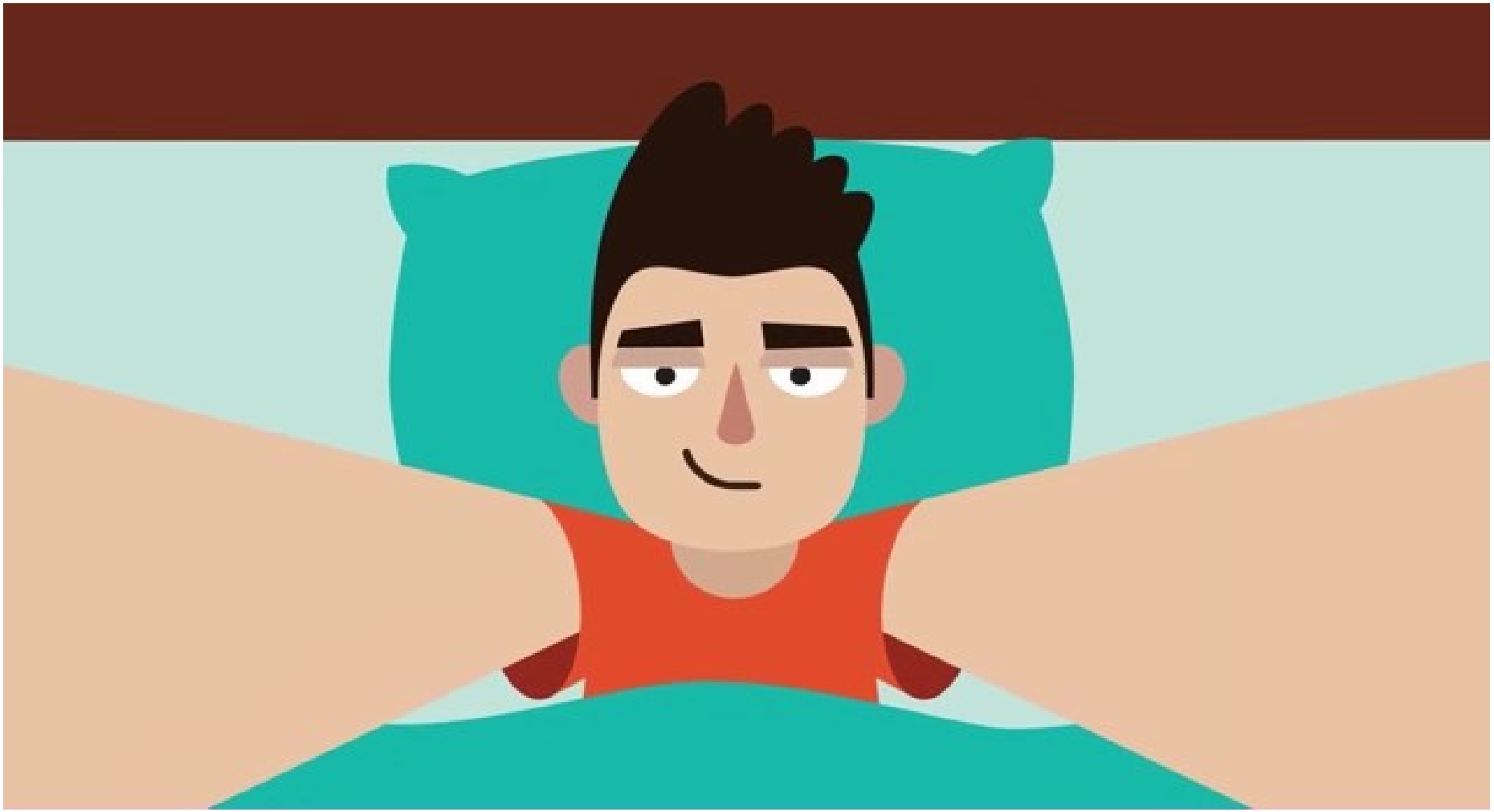
Oculta tu identidad y tu navegación en línea de muchas formas de vigilancia de Internet.

También ser útil como un medio seguro para promover la libertad en Internet, y eludir la censura y las restricciones electrónicas

https://www.torproject.org/projects/torbrowser.html.en#downloads

navegación segura con TOR

https://www.youtube.com/watch?v=Sz_J6vJ4MYw



-autodefensa digital-
glosarios de términos

Glosario de Surveillance Self-Defense
en
https://ssd.eff.org/es/glossary

Glosario de Security in a Box
en
https://info.securityinabox.org/es/glossary

Fuentes consultadas
y para consultar

(1) https://ssd.eff.org/es/
(2) https://emailselfdefense.fsf.org/es/
(3) https://info.securityinabox.org/es/
(4) http://wiki.hacktivistas.net/
(5) https://we.riseup.net/hacklab+asamblea/seguridad_informatica
(6) http://sursiendo.com/blog/tag/materiales/

seguimos platicando...

http://sursiendo.com/blog/

jes@sursiendo.com

@Sursiendo

@HabíaUnaJes

Sursiendo

2015