**Seguridad, Privacidad y protección**

En la actualidad la mayoría de las personas tenemos un **perfil digital**. Según se van añadiendo responsabilidades en nuestra vida (cursos, clases, trabajos...) existe más información digital sobre nosotros. Cuando utilizamos nuestro móvil, tablet, ordenador, también.

| ¿Sabrías decir qué es un perfil digital? |
|---|

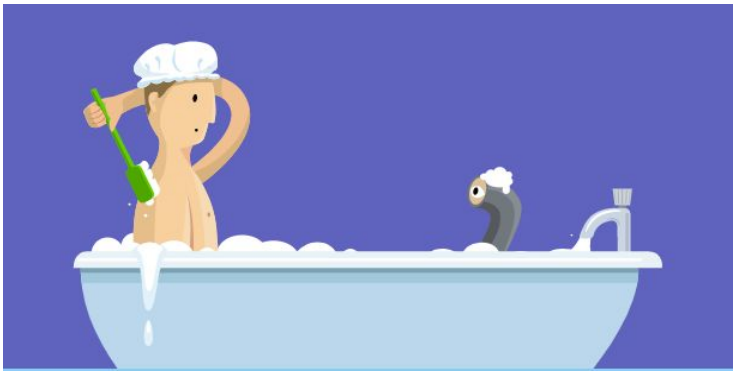
Aunque la mayor parte de los usuarios lo desconozca, éstos tienen una serie de derechos en internet. Muchas empresas e incluso gobiernos incumplen estos derechos, jugando con los límites legales y el desconocimiento de los usuarios. Sin embargo, existen individuos y asociaciones dedicadas a protegerlos. El consejo Europeo reúne dichos derechos en un documento público, pero en resumen, **¿Qué derechos más importantes debe tener un usuario de internet?**

| ¿Qué derechos crees que debería tener un usuario corriente en internet? |
|---|

***"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**

- **Derecho a la privacidad**. Tus datos son tuyos, y aunque no tengas nada que esconder, es importante comprender que existe. Tampoco nos gustaría vivir en una casa transparente, ¿verdad? con internet ocurre lo mismo.
- **Derecho al anonimato**. Está muy relacionada con la anterior. Un usuario tiene derecho a permanecer anónimo mientras navega, y esto no es o no debería ser ilegal. Hay determinadas herramientas que ayudan a esto.
- **Nuestros datos personales** sólo se ceden bajo petición legal o consentimiento. Con esto juegan muchas empresas que ofrecen servicios "gratuitos" a cambio de estos datos. Esto no es un problema mientras seamos conscientes de por qué y cómo tratan nuestros datos.



Navegar seguro en internet

¿Qué información crees que guarda un navegador como Google Chrome de nosotros?

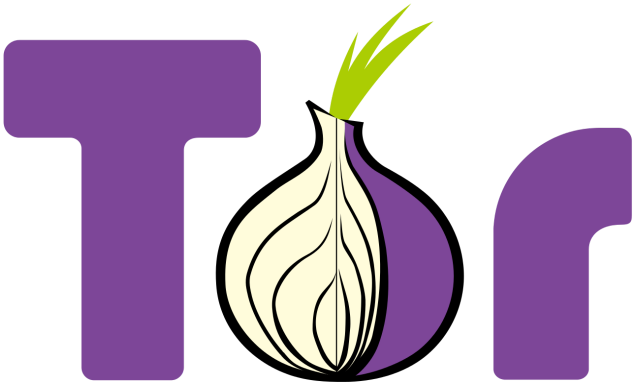
Vale, tenemos unos derechos, y queremos proteger nuestra información. ¿Cómo lo hacemos?

1. ¡Sentido común! Ojo con lo que publicamos en las redes sociales.
2. Navegador… buscador… ¿Seguros?

¿Qué diferencia hay entre navegador y buscador? ¿Conoces ejemplos?

¡Si! Existen muchos navegadores, algunos de los más famosos son Google Chrome, Internet Explorer, Mozilla, Opera… Todos sirven para conectarnos a nuestras páginas favoritas. Sin embargo debemos tener cuidado a la hora de escogerlos. **Internet explorer** está bastante desactualizado y tiene errores de seguridad que pueden comprometer nuestro ordenador; **Opera** es poco conocido pero en general funciona bien; **Google Chrome** tiene muchas opciones de extensiones, sin embargo funciona bajo las condiciones de Google, se basa en un navegador libre llamado Chromium; **Mozilla** tiene también opciones de extensiones, y tiene una política de privacidad algo mejor que Google Chrome.

Además de estos navegadores existe también **TOR**, un navegador que nos permite navegar de forma anónima por la red. **¿Cómo?** Nos permite hacernos pasar por otros ordenadores, y en lugar de ir directamente de tu ordenador a una web, hace un camino más largo por varios ordenadores, haciendote prácticamente irrastreable. Algunas personas se sienten más seguras consultando determinada información a través de TOR, o en países con mucho control y poco respeto por la privacidad.  Por sus cualidades tiene mala fama en algunos ambientes pero en realidad es una herramienta útil para periodistas, activistas y usuarios de todo tipo.



¿En qué ocasión un usuario querría utilizar TOR?

Sobre los buscadores, nos permiten encontrar páginas concretas, como cuando buscamos una receta en Google. Pero además de Google (famoso por tener un motor de búsqueda muy decente) existen otros. Entre la gama de buscadores, una alternativa bastante interesante es **DuckDuckGo**. Su motor de búsqueda es similar al de Google, solo que no guarda tus datos. Esto hace que las búsquedas sean “menos personalizadas” pero su política de privacidad es notable.


Probemos a hacer las siguientes búsquedas:

- Hola mundo
- list command linux

¿Qué ocurre? ¿Sabrías distinguir la funcionalidad “ahorro de clicks” aquí?

Además a veces nos conectamos a páginas web que pueden comprometer nuestros datos. ¿Te has fijado alguna vez en los links de internet? Por ejemplo…

```
https://duckduckgo.com/?q=hola+mundo&t=h_&atb=v99-2__&ia=web
```

Aquí, tenemos al inicio https. Eso significa que entre tu ordenador y la página se están hablando de forma encriptada, y un tercero no puede entender lo que ocurre si vigilara. Sin embargo….

```
http://http://www.ugr.es/
```

Comienza por http. Esto significa que entre tu ordenador y la web se están hablando sin encriptar y cualquiera que vigile la comunicación sabe lo que ocurre.

¡Oh no! ¿Y cómo lo solucionamos? Para esto existe una extensión llamada **HTTPS EVERYWHERE** que nos permite emular la privacidad del https en todas partes. Es gratis, es libre y funciona en varios navegadores.

Instalemos la extensión en el navegador. ¿Sabrías como?

Algunas páginas utilizan algo llamado “cookies” (galletas en inglés), las cookies básicamente guardan información del usuario en su navegador para agilizar la página. Es como si fuera una chuleta para la página web y que no tenga que recordarlo todo. Esto es genial, pero tiene su peligro, si no borramos esa información alguien podría robarla, sin embargo es difícil recordar borrarlo todo el tiempo. ¡No pasa nada! para eso tenemos **PRIVACY BADGER**, desarrollado por los mismos que **HTTPS EVERYWHERE.** La extensión es un “mapache” (o así lo representan) que se “come” las “cookies” automáticamente.

Instalemos también Privacy Badger

**Incluso si usamos todo esto, a veces nuestra información y nuestros datos están comprometidos**, por ello es recomendable el uso de comunicación segura. Por ejemplo, tener un correo electrónico alternativo no intrusivo (que no requiera datos como nombre, dni, otro correo, móvil...) y encriptar nuestros mensajes.

Uno de los correos gratuitos más seguros es **PROTONMAIL**. Son respetuosos con los datos y encriptan los mensajes entre los propios usuarios de protonmail. Por conveniencia de la clase, hemos creado uno:

- INSERTAR AQUÍ DATOS DE SESIÓN DE PROTONMAIL -

Pero además podemos encriptar nuestro mensaje para mayor seguridad. Existen dos tipos fundamentales de encriptación, los de **llave única** y los de clave **pública-privada**.

**En los de llave pública**, se utiliza un algoritmo que queramos y convertimos el mensaje en algo que no se puede leer a simple vista. Sin embargo, si alguien tiene la llave (una contraseña), puede deshacer el algoritmo y ver el mensaje.

Vamos a probar a encriptar el siguiente mensaje con diferentes algoritmos:

*Ser o no ser, esa es la cuestión.*

Para ello usaremos esta web: https://codebeautify.org/encrypt-decrypt

**Clave pública-privada**, es más segura que la anterior, también un poco más compleja. Primero es como el proceso anterior, encriptamos un mensaje cualquiera. pero en lugar de sacar una sola llave para poder descifrarlo, se sacan dos llaves distintas.

Con la primera llave se pueden cifrar mensajes, esa es pública y puede tenerla quien tu quieras (incluso publicarla para todo el mundo).
La segunda llave solo la tienes tú, y nada más que tú, y sirve para descifrar todos los mensajes que se hayan hecho con la primera llave.

Cualquier persona que tenga la primera llave puede crear mensajes secretos, pero solo tú, con la llave privada puedes leerlos. De este modo solo la persona que lo ha creado y tú sabéis el contenido del mensaje, y nadie más, puesto que con la clave pública no se puede descifrar, sólo cifrar.

Crea un par de llaves en esta web : https://sela.io/pgp/ y manda un mensaje a CORREODELPROFESOR (a ser posible de protonmail) con tu cuenta de protonmail.