Actividad 14. Seguridad en navegadores y navegación segura

1. Busca información en los artículos indicados y en otros sitios sobre la seguridad y los navegadores y la navegación segura

2. Elabora un documento explicando las opciones de seguridad en los navegadores

3. Indica los navegadores más seguros

4. Elabora una lista de acciones y elementos que hay que tener en cuenta para una navegación segura

OPCIONES DE SEGURIDAD EN LOS NAVEGADORES:

1. ***Configuraciones Básicas de la Seguridad:***

- ***Actualizaciones Automáticas***: Mantener el navegador siempre actualizado para protegerse contra vulnerabilidades y exploits recientes.
- ***Protección contra Phishing***: Habilitar opciones que detectan y bloquean sitios web fraudulentos que intentan robar la información personal.
- ***Bloqueo de Cookies de Terceros***: Restringir cookies de terceros para evitar el seguimiento no deseado por parte de anunciantes y otras entidades.

2. ***Configuraciones de Privacidad:***

- ***Modo Incógnito***: Navegar en modo incógnito para evitar que el navegador guarde el historial de navegación y las cookies.
- ***Gestión de Contraseñas***: Utilizar gestores de contraseñas integradas o externas para crear y almacenar contraseñas seguras.
- ***Permisos de Sitios Web***: Revisar y ajustar los permisos que los sitios web tienen para acceder a datos como ubicación, cámara y micrófono.

3. ***Extensiones y Herramientas de Seguridad:***

- ***Extensiones de Bloqueo de Anuncios***: Instalar extensiones como uBlock Origin para bloquear anuncios y posibles malware.
- ***Herramientas de Encriptación***: Usar extensiones para encriptar datos y asegurar las comunicaciones en línea.

4. ***Características Avanzadas:***

- ***Sandboxing***: Navegadores como Google Chrome usan sandboxing para aislar procesos y prevenir que malware afecte al sistema.
- ***Listas de Bloqueo de Malware***: Activar listas de bloqueo de sitios conocidos por distribuir malware.

NAVEGADORES MÁS SEGUROS EN 2024:

1. ***Google Chrome***: Destaca por su actualización constante y robustas características de seguridad como el sandboxing y protección contra phishing.
2. ***Mozilla Firefox***: Ofrece configuraciones avanzadas de privacidad y extensiones de seguridad. Es conocido por sus opciones de personalización de seguridad.
3. ***Microsoft Edge***: Integración de herramientas de seguridad avanzadas y actualizaciones regulares para proteger contra amenazas emergentes.
4. ***Safari***: Buenas características de privacidad y seguridad, especialmente en dispositivos Apple. Bloqueo efectivo de cookies y rastreadores.
5. ***Brave***: Enfocado en la privacidad desde el inicio, bloquea anuncios y rastreadores por defecto, y ofrece opciones de navegación segura.

ACCIONES Y ELEMENTOS PARA UNA NAVEGACIÓN SEGURA:

1. ***Mantén el Navegador Actualizado***:
   - Asegúrate de que tu navegador esté siempre actualizado para beneficiarte de las últimas correcciones de seguridad y mejoras.
2. ***Configura la Privacidad Adecuadamente***:
   - Ajusta la configuración de privacidad para limitar el seguimiento y proteger tu información personal, incluyendo gestionar las cookies y permisos de sitios web.
3. ***Usa Contraseñas Fuertes y Únicas***:
   - Implementa contraseñas seguras y utiliza un gestor de contraseñas para mantenerlas seguras y únicas para cada cuenta.
4. ***Activa la Autenticación en Dos Pasos***:
   - Activa la autenticación en dos pasos para cada una de las cuentas en línea. Así, se añade una capa extra de protección.
5. ***Instala Extensiones de Seguridad***:
   - Utiliza extensiones para bloquear anuncios, proteger contra rastreadores y gestionar contraseñas.
6. ***Revisa los Permisos de los Sitios Web***:
   - Controla los permisos que se conceda de los sitios web (acceso a la ubicación, cámara o micrófono)
7. ***Navega con Modo Incógnito***:

- Utiliza el modo incógnito para evitar que el navegador guarde el historial y las cookies, aunque esto no nos hace anónimos en la web.

8. ***Habilita la Protección contra Phishing***:
   - Hay que estar seguros de la protección contra phishing y sitios web peligrosos esté activada para recibir alertas de seguridad.
9. ***Revisa la Seguridad de las Conexiones Web***:
   - Asegúrate de que las conexiones a sitios web sean seguras, verificando que la URL comience con "*https://*".