Día Internacional de Internet Segura: medidas para la navegación segura

Con motivo de la celebración, hoy 6 de febrero, del **Día Internacional de Internet Segura**, y en colaboración con el Responsable de Seguridad de la Información de la Universidad de Granada, se recuerda la importancia de mantener unos hábitos básicos para una navegación segura al objeto de evitar el robo de datos, ataques de malware (especialmente de ransomware), ataques de ingeniería social o denegación de servicio.

En el **Decálogo de Ciberseguridad** (Web UGR->Secretaria General->Seguridad de la Información->Decálogo de Ciberseguridad) se recogen algunas medidas que recordamos de nuevo y extendemos:

- Generales:

- Actualización regular del software, especialmente el navegador seguro.
- Usar VPN para cifrar y redirigir el tráfico de cara proteger nuestros datos.
- Utilizar gestor de contraseñas:
  - No almacenar contraseñas de forma predeterminada por medio del navegador y usar gestores con un sistema de cifrado robusto.
  - En caso de que sea necesario almacenarlas en el navegador hacer uso de la llave maestra robusta para cifrar el almacén de contraseñas.
  - Por supuesto tener una contraseña única para cada sitio, utilizar doble factor de autenticación donde sea posible.
  - Relativas a la propia navegación:

- Revisar las opciones de privacidad y seguridad del navegador. Especialmente interesantes son las opciones para: no aceptar cookies de terceros, bloquear pop-ups, evitar la sincronización de contraseñas, evitar el autocompletado de formularios, borrar archivos temporales y cookies al cerrar el navegador, bloquear la auto-localización, etc.

- Elegir comunicación https, frente a http, y verificar que está activo el cerrojo de navegación segura a la izquierda de la barra de navegación.

- No hacer caso a las solicitudes de rastreo de los sitios web visitados.

- Limpiar la caché y las cookies no deseadas del navegador. Otra posible opción sería utilizar dos navegadores separados: uno para uso personal y otro laboral.

- Usar navegación privada para proteger la información privada y evitar el rastreo.

- Valorar el uso de extensiones o complementos adicionales que añaden funcionalidad no contemplada en el navegador:

o Bloquear anuncios (Ad Blockers), banner publicitarios o técnicas de rastreo de la navegación.

o Utilizar pluging para verificar la confianza del sitio web al que deseamos acceder, o utilizar herramientas online para ellos, por ejemplo: Norton safe web (https://safeweb.norton.com/), TrendMicro Site safety (https://global.sitesafety.trendmicro.com/index.php), mxtoolbox (https://mxtoolbox.com/), o urlvoid (https://www.urlvoid.com/).

o Tener especial cuidado con las URLs acortadas (usar validadores de URL: Unshorten.it (https://unshorten.it), Urlex.org (https://urlex.org), Unshorten.net (https://unshorten.net), Unshorten.me (https://unshorten.me), o Unshorten.xyz (https://unshorten.xyz).

Más información:

https://secretariageneral.ugr.es/informacion/servicios/seguridad-informacion

José Antonio Gómez Hernández
Responsable de Seguridad de la Información
Universidad de Granada
Cuesta del Hospicio s/n
18071 - Granada (Spain)
@email

Enviado el 6 febrero de 2024 a infougr@listas.ugr.es