



UNIVERSIDAD DE GRANADA

Vicerrectorado de
Estudiantes y Vida
Universitaria

6 de febrero, Día Internacional de Internet Segura.

06/02/2024

La Secretaria General de la Universidad de Granada informa, 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

10 consejos de ciberseguridad

Usa antivirus
No enlentece el sistema y evita un alto porcentaje de problemas.

Gestiona tus contraseñas
Deben ser fuertes y distintas en cada plataforma. Usa un gestor de contraseñas (no el del navegador) y doble factor de autenticación.

Haz copias de seguridad
en dispositivos externos, pero que no estén siempre conectados, para que nadie pueda tener acceso a ellos y borrarlos o dañarlos.

No dejes tus dispositivos desatendidos
Bloquea el ordenador cuando no este en uso y establece contraseña para el salvapantallas.

Mantén actualizado
tu sistema operativo y aplicaciones. De esta manera estará más seguro y será más complicado atacarlo.

Aplicaciones seguras
Instala las aplicaciones que provengan solo de fuentes de confianza: páginas web y tiendas oficiales.

Usa cifrado de datos
para proteger la información en todos tus medios extraíbles y tu ordenador.

Cuidado con el phishing
Cuando recibas un correo verifica el emisor, lee bien el texto, nunca des datos personales, ni contraseñas, no pinches enlaces y verifica los adjuntos antes de abrírlos.

Minimiza tu huella digital
evitando dar información personal en redes sociales. No uses el usuario/contraseña de la UGR en servicios externos a ella.

Navega de forma segura
Ten cuidado cuando pinchas un enlace o descargas un archivo. Verifica la reputación del sitio web al que vas a acceder.

Si tienes alguna duda contacta con el servicio de seguridad: csirc@ugr.es

10 consejos de ciberseguridad

Usa antivirus
No enlentece el sistema y evita un alto porcentaje de problemas.

Gestiona tus contraseñas
Deben ser fuertes y distintas en cada plataforma. Usa un gestor de contraseñas (no el del navegador) y doble factor de autenticación.

Haz copias de seguridad
en dispositivos externos, pero que no estén siempre conectados, para que nadie pueda tener acceso a ellos y borrarlos o dañarlos.

No dejes tus dispositivos desatendidos
Bloquea el ordenador cuando no este en uso y establece contraseña para el salvapantallas.

Mantén actualizado
tu sistema operativo y aplicaciones. De esta manera estará más seguro y será más complicado atacarlo.

Aplicaciones seguras
Instala las aplicaciones que provengan solo de fuentes de confianza: páginas web y tiendas oficiales.

Usa cifrado de datos
para proteger la información en todos tus medios extraíbles y tu ordenador.

Cuidado con el phishing
Cuando recibas un correo verifica el emisor, lee bien el texto, nunca des datos personales, ni contraseñas, no pinches enlaces y verifica los adjuntos antes de abrírlos.

Minimiza tu huella digital
evitando dar información personal en redes sociales. No uses el usuario/contraseña de la UGR en servicios externos a ella.

Navega de forma segura
Ten cuidado cuando pinchas un enlace o descargas un archivo. Verifica la reputación del sitio web al que vas a acceder.

Si tienes alguna duda contacta con el servicio de seguridad: csirc@ugr.es

ransomware), ataques de ingeniería social o denegación de servicio.

En el **Decálogo de Ciberseguridad** se recogen algunas medidas que recordamos de nuevo y extendemos:

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

+Info