Las redes sociales y los argentinos: cómo se usan y cuáles son los errores más comunes

Desde hace 12 años, cada 30 de junio se celebra el **Día Mundial de las Redes Sociales**, una iniciativa del portal Mashable debido al crecimiento exponencial de las plataformas. Cada país tiene sus **propios usos** y medidas de cuidado **cibernéticas**. Particularmente, **Argentina cuenta con más de 34,46 millones de usuarios y se espera que la cifra supere los 40 millones para el 2026**, acompañado de mayores **beneficios y riesgos**.

«Nuestro país cuenta con 35 millones de usuarios de Internet, aumentando un 2% con respecto al último año, y **34 millones de usuarios activos en medios sociales**, teniendo un aumento de casi 7% a diferencia de abril 2019?, aseguró **Olga Cavalli**, subsecretaria de Tecnologías de la Información perteneciente a la Secretaría de Innovación Tecnológica.

Según un **estudio**-citado por Brand Partners-, se espera que la cifra de usuarios que utilizan las redes sociales supere los **40 millones para el 2026**. Aquello conlleva una mayor atención hacia los **ciberdelitos**, es decir, a las conductas ilícitas / ilegales

que **vulneran derechos o libertades de las personas** y utilizan un dispositivo informático como medio para la comisión del mismo o fin.

Por lo tanto, resulta esencial ser conscientes de las **políticas de prevención, detección y cuidado frente a los incidentes de seguridad informática**. Debemos priorizar la **ciberseguridad** que -según la compañía IBM- es la práctica de **proteger** los sistemas importantes y la información confidencial de los **ataques digitales**. Las medidas de seguridad cibernética están diseñadas para **combatir las amenazas contra sistemas en red y aplicaciones**.

Redes sociales.

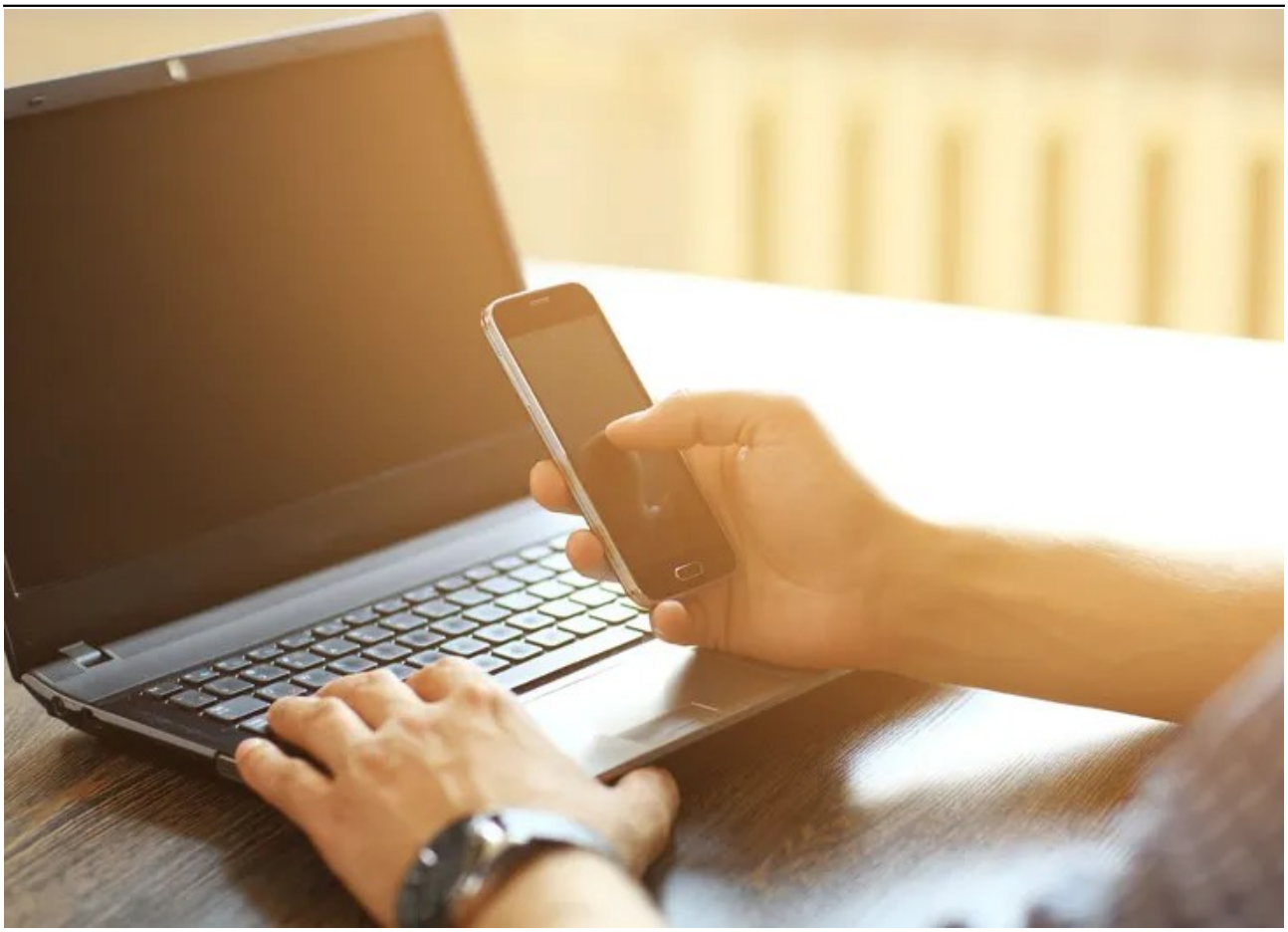
Cuáles son las redes sociales más utilizadas por los argentinos

Según la empresa WeAreSocial, Argentina tiene **un uso particular y un**

posicionamiento con respecto a la cantidad de usuarios –**16 a 64 años**– que pertenecen a cada espacio. Teniendo en cuenta que un argentino invierte al día **3 horas y 11 minutos** usando redes sociales, las plataformas más utilizadas son:

- **YouTube**: 95%.
- **WhatsApp**: 92%.
- **Facebook**: 90%.
- **Instagram**: 76%.
- **FB Messenger**: 62%.
- **Twitter**: 52%.
- **Pinterest**: 44%.
- **LinkedIn**: 31%.
- **TikTok**: 13%. Actualmente, está en tendencia y no supera los **4,5 millones de usuarios activos** en promedio.

Pero si salimos de las redes tradicionales, en 2021, **WhatsApp** fue la más utilizada por los argentinos. Y se esperan los mismos resultados para este año. Seguido, siguen **Instagram y Facebook** como las preferidas, y con porcentajes de uso superando el **80% de los usuarios de Internet**, según datos relevados por la **Cámara Argentina de Internet** (CABASE).



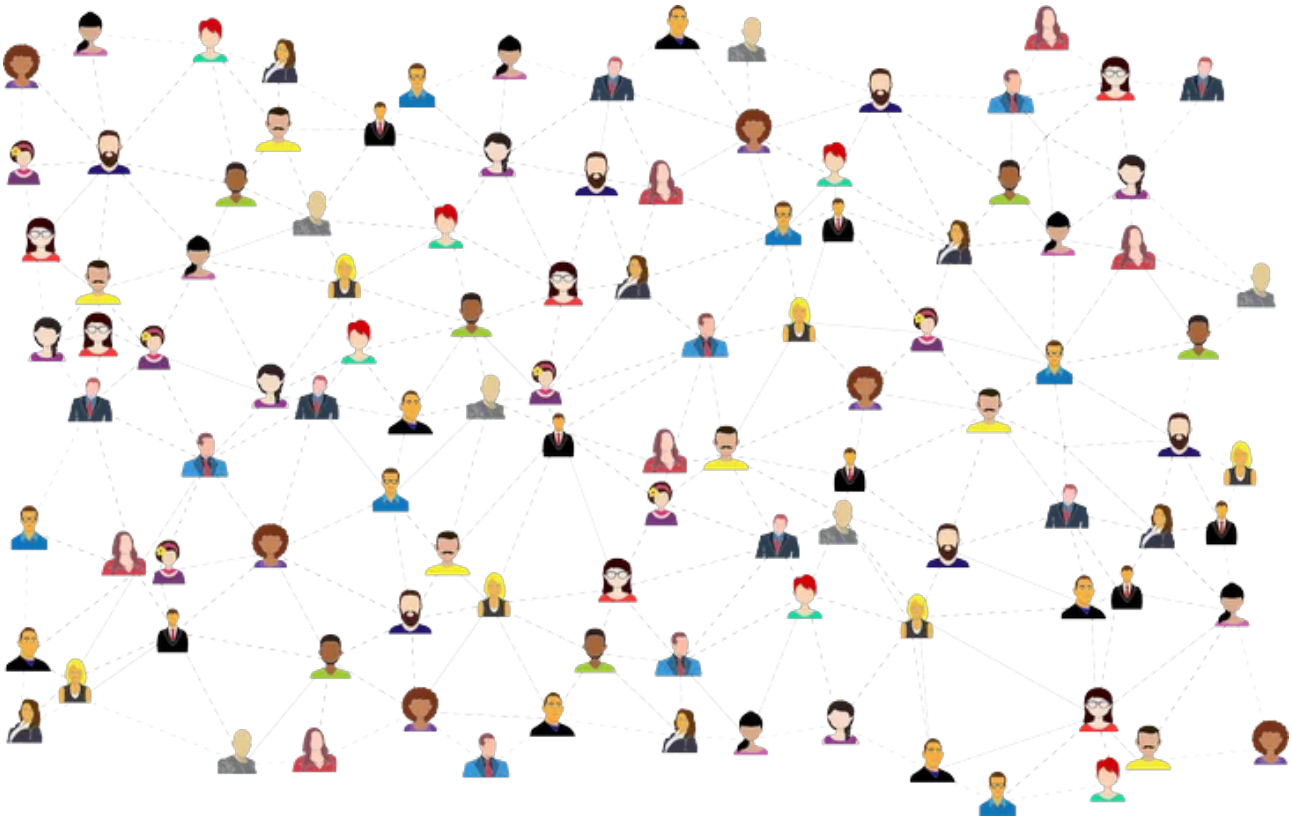
Smartphone.

Las redes sociales y los argentinos: cuáles son los errores más comunes

«El error más típico que sufrimos todos los usuarios de redes sociales es el **desconocimiento** de lo que sucede cuando las utilizamos, sumado a la **sencillez** nos brindan para su uso», dijo **Abel Decaroli**, Director de Prevención en Seguridad de Sistemas y Redes Informáticas.

Y ejemplifico: «Al recibir un email o una nueva solicitud de contacto, tenemos **confianza extrema** y aceptamos cualquier archivo, **sin siquiera corroborar o preguntarnos cuál es el fin de interactuar**. También ocurre con las **configuraciones de privacidad** que

generalmente no utilizamos o las dejamos como están por defecto, **perdiéndonos una herramienta valiosa que nos puede ayudar a minimizar o prevenir un incidente de seguridad informático**«.



Por su parte, **Check Point® Software Technologies Ltd.**, un proveedor de soluciones de ciberseguridad a nivel mundial, destaca los cuatro principales **factores de riesgo** a tener en cuenta para **mantenerse seguro al usar las redes sociales**:

Compartir información personal

Resulta ser un **error muy común y peligroso** que ocurre todos los días en las redes sociales, ya que los ciberdelincuentes buscan robar información personal. Y, armados con aquellos datos, pueden lanzar múltiples **campañas de phishing**-suplantación de identidad- o incluso quedarse con tu **dinero**.

También vale mencionar que la mayoría de las personas que usa el **mismo usuario y clave para diferentes plataformas** corren un riesgo mayor: al robar las credenciales de una, los hackers tienen un **acceso potencial** a todas las cuentas. Por lo tanto, es vital que **no compartas datos personales**, que utilices **diferentes contraseñas** y actives el **doble factor de autenticación** -siempre que sea posible- para minimizar el daño en caso de ser víctima de un ataque.

Contraseña.

Abrir correos electrónicos de restablecimiento de contraseña no solicitados

Existen tantas plataformas que es muy sencillo pensar que en algún momento puede haber algún incidente con alguna y es ahí cuando **los hackers se aprovechan**. Si recibís un correo electrónico pidiéndote que cambies tu contraseña, incluso si no lo solicitaste, generalmente, **el primer impulso es hacer clic en el enlace y restablecerla**.

Pero es **peligroso**, ya que podes dar **acceso completo** de tu cuenta al ciberdelincuente.

Para evitarlo, tendrás que dirigirte a la página de la plataforma y luego deberás **renovar tu contraseña** desde el propio sitio (y finalmente hacer lo mismo para otras cuentas con la misma clave).

Gentileza: Pexels.

Hacer clic en cualquier enlace

Los ciberdelincuentes suelen utilizar enlaces para redirigir a los usuarios a **sitios maliciosos**. Los links pueden aparecer en forma de **correo electrónico o SMS**. Si recibís un enlace similar, la mejor manera de protegerse es **ir al sitio en cuestión**, a través del navegador habitual, y verificar si hay mensajes, en lugar de hacer clic en un **enlace de dudosa procedencia**.

No comprobar las URL

Otro truco que usan los hackers para robar datos es **cambiar una URL para que parezca genuina**. Permiten que el usuario visite el sitio web creyendo que es **confiable**. Por ejemplo, solicitan un cambio de contraseña para luego redirigirlos a una **página clonada** y así **robar tanta información como sea posible**.

Hacker.

Pixabay

El reporte **“Brand Phishing” de Check Point** arrojó que la red social **LinkedIn** domina por primera vez aquellos ataques, representando **más de la mitad (52%) de todos los intentos de phishing** en el primer trimestre del año. Por eso, siempre hay que verificar que la web disponga de **certificado de seguridad SSL**. Si es así, debería decir: **https://**.

La tecnología permite que cualquier **información confidencial** que se envíe entre dos sistemas quede **protegida** y además evita que los ciberdelincuentes **accedan a los datos que se transfieren**.

Phishing.

Cómo protegerse de los incidentes informativos

Frente a los incidentes informativos, según Decaroli, «si bien hay muchas recomendaciones y acciones que podemos tener para protegernos, lo fundamental es **entender y saber qué se quiere hacer dentro de una red**, para qué la utilizo y con quiénes me comunico». Y -continuó- «si bien**nunca nadie puede estar al 100% protegido dentro de Internet**, con esta consciencia, seguramente minimicemos en gran medida los posibles incidentes que podamos sufrir o causar».

Y el director brindó algunos consejos a la hora de navegar tanto en las redes sociales como en Internet:

- «Nunca contestes con **datos sensibles** algún pedido que no hayas iniciado. Casi todas las comunicaciones espontáneas suelen iniciarse para realizar una **estafa virtual o conseguir información**«.
- «Cuando no la necesites, se recomienda mantener tu **webcam desconectada o tapada**«.
- «Evita en la medida de lo posible aceptar solicitudes de gente que **no conozcas en la vida real**. Si lo haces, recordá que dentro de Internet es muy fácil **hacerse pasar por otra persona**«.

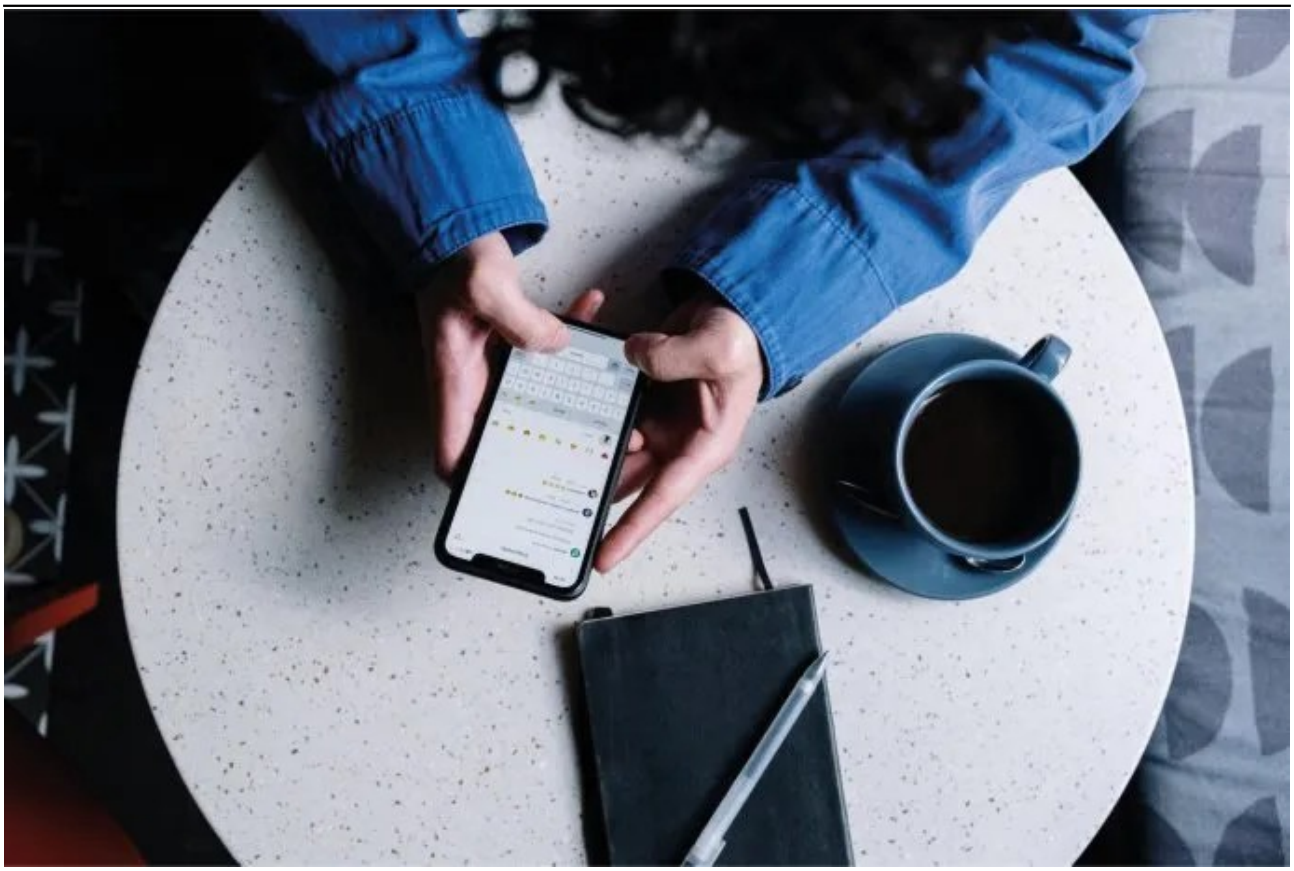
Foto Unsplash

En esa misma línea, Cavalli expresó que **«la concientización sobre cómo prevenir incidentes es fundamental para el uso de las redes sociales»**. Y destacó la **doble autenticación**: «Es fundamental, ya que agrega una **barrera más de seguridad** que además no es compleja de configurar, pero muchas personas no lo hacen por desconocimiento y terminan siendo un **perfil más vulnerable**«.

Otras de las recomendaciones son «**cambiar regularmente las claves**, evitar que sean obvias o fáciles de descubrir; hacer regulares **backups** (copia de seguridad) de la información almacenada en nuestros dispositivos; estar alertas y **no ingresar en links que resulten sospechosos**«.

Pexels

Por último, la subsecretaria aconsejó «activar las distintas **configuraciones de privacidad** que ofrecen las redes sociales», además de «utilizar elementos que ayuden a **proteger la seguridad**, como los **antivirus y firewalls**«.



Banco de fotos

Qué hacer si fuiste víctima de un incidente informativo

Desde **Innovación Tecnología** recomiendan, en materia sancionatoria, buscar asistencia, ayuda o asesoramiento en los siguientes sitios:

- Para **denunciar un delito informático**, concurrir a la comisaría más cercana, a la fiscalía especializada del tema o, en su defecto, a una común.
- Para consultar sobre los **derechos de las personas respecto a sus datos personales**, comunicarse con la Dirección Nacional de Protección de Datos Personales llamando al 011-3988-3968 o enviando un correo electrónico a datospersonales@aaip.gob.ar.
- Ante problemas relativos a **productos o servicios en Internet**, llamar a Defensa del Consumidor al 0-800-666-1518 o ingresando a la página del organismo.

- **Los servicios y las aplicaciones digitales** deben tener canales de denuncias u otras vías de contacto para realizar reclamos o quejas.

Fuente: Ámbito