El 68% de los argentinos utiliza las redes sociales como fuente de información, según un estudio

13/10/2021

Siete de cada diez argentinos, de entre 20 y 65 años de edad, recurrieron a las redes sociales para acceder a información durante los primeros 12 meses del confinamiento por la pandemia de coronavirus, según un estudio realizado por la empresa global de ciberseguridad y privacidad digital Kaspersky.

El estudio **“La infodemia y su impacto en la vida digital”**, desarrollado en conjunto con la empresa de investigación Corpa, registró una leve preferencia hacia estas plataformas entre las mujeres (74%) en comparación con los hombres (61%).

Para los investigadores, esta práctica es preocupante dado las consecuencias que puede tener en la privacidad, reputación y bienestar general, especialmente al considerar el fenómeno de

infodemia que se desató durante la pandemia.

Entre otros datos, el estudio revela que, entre marzo de 2020 y marzo de 2021, el 58% de los argentinos siguió consejos para el cuidado de su salud que leyeron en redes sociales.

Además, el 80% dijo que utilizó las redes sociales para mantenerse informado sobre el funcionamiento de servicios públicos y comerciales, tendencia que no ha pasado desapercibida por defraudadores y cibercriminales.

El director del Equipo de Investigación y Análisis para América Latina en Kaspersky, Dmitry Bestuzhev, explicó que **“cuanta más gente esté conectada a un servicio o plataforma, más atractiva es para los ciberdelincuentes”. “Por ejemplo, tan pronto como comenzaron las reglas de aislamiento, registramos un auge en los ataques de phishing -suplantación de identidad- a dispositivos móviles. Esto porque la mayoría de los usuarios recurrió a servicios en línea y aplicaciones a través de su Smartphone”**, detalló el experto.

Según el especialista, la sobrecarga y el ‘apagón’ mental provocados por la infodemia durante los meses de confinamiento hicieron a las personas más vulnerables a estas estafas.

Según Bestuzhev, el phishing es la táctica más utilizada en redes sociales por defraudadores.
De acuerdo con datos del Panorama de Amenazas en América Latina de Kaspersky, la lista de países de la región más afectados por phishing durante los primeros ocho meses de 2021 está liderada por:

- Brasil: 15,37%
- Ecuador: 13,36%
- Panamá: 12,60%
- Chile: 11,90%
- Colombia: 11,09%
- Perú: 10,30%
- Guatemala: 10,21%

• México: 9,41%
• Argentina: 9,17%
• Costa Rica: 7,64%

“El consumo de información en línea sucede rápidamente y a menudo pasa sin que los usuarios presten atención a los detalles, como la veracidad de la información, la fuente, y si lo que estamos leyendo tiene sentido”, explicó Bestuzhev.

El especialista resaltó que “la gente suele pensar y sentir que la información en estas plataformas es más personal y por eso suele creer en los mensajes que se propagan. Esto puede afectar a la privacidad, identidad y hasta el bienestar físico o emocional”.

“Por eso, es fundamental tomar tiempo para desconectarnos, procesar la información recibida y evaluar los riesgos que podamos enfrentar antes de tomar alguna acción”, agregó.

Cuidados en las redes sociales

Para evitar convertirse en víctima, Kaspersky recomienda:

• Mantener un equilibrio en el consumo de noticias para evitar sentirse saturado por la cantidad de información que se comparte en las redes sociales.

• Utilizar la función “ver / leer más tarde”, disponible en varias plataformas y navegadores, para que pueda despejarse y crear hábitos que beneficien su salud mental.

• Antes de compartir, comentar o darle “Me gusta” a una publicación en redes sociales, darse tiempo para procesar la información.

• Verificar que la fuente sea válida y contemplar las posibles consecuencias de incluir algún comentario, o en asociarse con el punto de vista presentado.

• Tener presente que el Internet lo recuerda todo y una acción

en un momento de rabia o emoción, puede traer consecuencias.

• Sospechar siempre de los enlaces recibidos por correos electrónicos, SMS, redes sociales o mensajes de WhatsApp, especialmente cuando la dirección parezca sospechosa o extraña.

• Verificar la dirección del enlace, especialmente si este busca redirigirlo a otro hipervínculo.

• Utilizar una solución de seguridad confiable que proteja todos sus dispositivos en tiempo real.