

Cómo los errores y descuidos de los usuarios exponen a los sistemas informáticos a potenciales ciberataques

Los riesgos en el mundo digital son más cotidianos y frecuentes de lo que las personas creen. Solo usando el navegador de Internet, sin necesidad de un programa especial, se puede acceder a datos personales -como cédula de identidad, nombres de usuario y claves- o a las cámaras de seguridad de empresas y casas.

La tecnología ha avanzado de manera veloz y los usuarios no siempre están conscientes de los riesgos. Por ejemplo, gracias a la calidad de las cámaras de celulares actuales, es posible imprimir en 3D las llaves de una casa, a partir de la imagen que alguien envió por WhatsApp.

Anuncio Patrocinado

Por eso, la responsabilidad del usuario y el autocuidado es fundamental en materia de ciberseguridad para cualquier sistema informático. Hellis Leiva, consultor de Orión, explica que muchas vulnerabilidades se originan en descuidos o errores que pudieron evitarse de manera sencilla.

Un error frecuente de los usuarios, tanto a nivel personal como en las empresas, es guardar sus contraseñas en lugares inadecuados, como notas adhesivas o archivos de texto, por ejemplo; o bien dejan abiertos accesos públicos de sus computadoras en la red o de equipos industriales en Internet. “Eso los deja expuestos a un potencial ataque”, señala el experto.



WAVM | PUBLICIDAD

AGENCIA DE PUBLICIDAD

- 🖨️ Impresiones
- 📱 Manejo de redes sociales
- 📺 Videos y fotografías profesionales

🗨️ **Conversemos por WhatsApp**

Otro ejemplo, es que “las personas dejan abiertas las cámaras de seguridad de sus casas o las empresas dejan acceso a éstas, por lo que desde un navegador se pueden ver las cámaras, quién entra o sale, horarios, rutinas, lo que resulta útil para un delincuente”.

Educación Digital

A juicio de Hellis Leiva, el origen de estos errores está en la falta de “educación digital” por parte de los usuarios, quienes no siempre son conscientes de lo importante que es cuidar sus datos y actúan de manera descuidada cuando reciben un correo potencialmente peligroso o descargan archivos de origen desconocido, cuyos efectos en el sistema informático pueden generar pérdida de información sensible y perjuicios económicos derivados de la contingencia.

Según un reporte de seguridad en Latinoamérica 2022, realizado por ESET, el 48% de los encuestados afirmó haber sufrido un incidente de ciberseguridad. Otro 36% indica que el presupuesto asignado al área de ciberseguridad aumentó con respecto al año anterior, mientras que el 63% considera que no es suficiente.

“Las personas deben ser conscientes de lo que hacen en el mundo digital. Deben estar atentos a los riesgos y entender que lo que se hace o muestra en internet es igual de

Cómo los errores y descuidos de los usuarios exponen a los sistemas informáticos a potenciales ciberataques

importante que otras actividades personales. De eso se trata el autocuidado digital”, expresó Leiva.

Para ello, es recomendable mantener actualizados los softwares, no utilizar conexiones wifi públicas, usar siempre antivirus y un cortafuego, tener contraseñas fuertes, utilizar la autenticación de dos factores o de varios, proteger la información personal y utilizar dispositivos móviles de manera segura.

y tú, ¿qué opinas?