Pese a ciberseguridad, descuidos de usuarios ponen en riesgo su privacidad: INAI

Los ciberataques se valen de diversas estrategias y tipos de malware o software, y este tipo de agresiones son cada vez más numerosas, sofisticadas y peligrosas.

A pesar de las diferentes herramientas que existen actualmente para protegerse de ataques cibernéticos, los descuidos de los usuarios de internet en sus dispositivos conectados a internet siguen poniendo en riesgo sus datos personales y su privacidad, advirtió el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En el marco de la conmemoración del Día Internacional por una Internet Segura, que se celebra cada año el segundo martes de febrero, el INAI emitió una serie de recomendaciones para que los usuarios de la red conozcan los riesgos que implican el uso de las tecnologías y las nuevas actividades cotidianas que se realizan en línea, como el teletrabajo y la educación a distancia.

"La seguridad en internet se ha constituido como un reto tanto para las instituciones públicas y privadas como para la población en general, en el contexto de la pandemia de **covid-19,** debido al incremento del número de dispositivos que se conectan a las redes empresariales y tienen acceso a los datos corporativos, complicando la ciberseguridad en el ámbito laboral y el doméstico", aseguró el INAI en un boletín. **El Día Internacional por una Internet Segura** tiene el propósito de informar y educar en un uso responsable, respetuoso, crítico y creativo de la red, así como de recordar la importancia de proteger los derechos de la infancia en internet. El instituto explicó que los ciberataques se valen de diversas estrategias y tipos de **malware o software** malicioso, por lo que este tipo de agresiones son cada vez más numerosas, sofisticadas, peligrosas y masivas, lo que pone en riesgo no sólo los datos de las empresas sino la privacidad de la población, **particularmente de las niñas, niños y adolescentes.**

Entre las recomendaciones emitidas por el INAI, están: Revisar la configuración de las aplicaciones a través de las cuales accede a Internet y sus servicios. Es ideal **contar con cifrado de extremo a extremo.** Usar el modo incógnito reduce los datos que se comparten con el navegador. No guarda información sobre páginas web, ni historial, caché web, contraseñas, información de formularios, cookies u otros datos de sitios web, además borra archivos temporales cuando se finaliza la sesión. Generar contraseñas seguras. Esto se logra conformándolas con palabras aleatorias, números y signos.

Es recomendable cambiarlas frecuentemente. **Usar la autenticación de dos factores.** Con esto, al tratar de ingresar a una cuenta se envía un código de verificación mediante una aplicación móvil o SMS, como un mecanismo para confirmar la identidad de la persona usuaria, lo que dificulta enormemente los ciberataques. Actualizar sistemas operativos y aplicaciones. Considerando que las versiones antiguas tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en el programa, mientras que las recientes suelen incluir parches de seguridad. **Ser cauteloso con las redes inalámbricas gratuitas.** Son utilizadas por los ciberdelincuentes para obtener datos, por lo que pueden usarse para navegación intrascendente y ocasional, nunca para servicios financieros como banca online o aquellos que requieran autenticación real de usuario. **Utilizar VPN** para mejorar la privacidad. Estos sistemas ocultan la dirección IP del usuario y redirigen el tráfico a través de un túnel cifrado. **Realizar copias de seguridad** para proteger la información personal y corporativa de un equipo informático. **Evitar la instalación de aplicaciones de sitios no seguros.** La apertura de correos electrónicos o archivos adjuntos no solicitados que llegan de redes sociales o aplicaciones de mensajería. Instalar antivirus confiables y prestar atención a los avisos sobre sitios inseguros.

Autor: RAFAEL MONTES
Fuente de información: www.milenio.com