Día Internet Segura: consejos para prevenir fraudes en llamadas y redes sociales

7 febrero, 2023

Las estafas virtuales están a la orden del día. Mutan en modalidad y formas de contacto Cómo identificarlas para no caer en robos.

Cada segundo martes de febrero se celebra, desde 1997, “El Día de Internet Segura”, para impulsar, informar y educar un uso responsable, respetuoso, crítico y creativo de la red. Actualmente, estar actualizados en materia de seguridad para evitar caer en estafas es indispensable ante los números alarmantes de estos hechos.

Los últimos estudios del Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales de la Universidad Austral (Ocedic), en la Argentina en 2022 se registraron 4.800 fraudes mensuales promedio, un aumento casi del 200% respecto al año anterior.

Estafas en Whatsapp, phishing, usurpación de identidad y “cuento del tío 2.0”, son las diversas modalidades de estos robos, que recaudaron un monto aproximado de $1.200 millones.

Brindar apoyo y seguridad a los usuarios, se convirtió en una misión de gran importancia para Apex America, líder en Customer Experience en América Latina: “A partir de una iniciativa de aprendizaje y concientización que lleva más de un año en Apex, buscamos modificar actitudes y percepciones, tanto organizacionales como individuales, con el fin de desarrollar en los usuarios y usuarias una idea de importancia de la seguridad”, cuenta Carolina Marconetto , CTO de la compañía.

Para ayudar a reforzar la seguridad al momento del contacto con los centros de atención, brindan consejos para evitar fraudes en llamadas:

Si recibís una llamada de una entidad y querés validar su veracidad, debés saber que nunca te solicitarán: información confidencial como nombres de usuario o claves; que compartas códigos de verificación o numéricos enviados a tu teléfono/correo; que te dirijas a una sucursal bancaria con un código/cbu para realizar una transacción; que valides, compartas o realices acciones de manera urgente.

Las llamadas pueden ser utilizadas para validar información. Pero desconfiá de llamados que te soliciten brindar datos nuevos. En este último caso, es recomendable: no compartir información personal, agradecer la llamada y cortar la comunicación, contactarse con el canal oficial de la organización buscando la página oficial en el navegador y validar la veracidad de la llamada o mensaje recibido.

Asegurate de estar contactando el sitio oficial de la entidad. La clonación de páginas web es una modalidad que está en aumento, a simple vista tienen los mismos datos que el sitio oficial. Por eso: buscá el nombre de la compañía en tu

buscador y evitá ingresar a páginas web desde un link en un correo o mensaje. Verificá que el sitio web comienza por HTTPS y que cuente con un candado de seguridad a la izquierda de la URL.

Tus datos protegidos. La ley nacional 25.326 otorga al ciudadano la potestad de conocer quién, cómo y para qué se utilizan sus datos personales registrados en archivos y bancos de datos, tanto públicos como privados. Podés ingresar al sitio web de la Dirección Nacional de Protección de Datos Personales para conocer la información que guarda una determinada entidad sobre tu persona. Al acceder a estos datos, tendrás la posibilidad de corregirlos, modificarlos y/o eliminarlos.

Ran Security, empresa líder en ciberseguridad, partener de Apex America en gestión de ciberseguridad, repasa las medidas de protección a la hora de utilizar Internet:

Evitá utilizar redes WiFi públicas. Es recomendable que utilices la conexión de datos de tu teléfono cuando te conectes a internet. De ser indispensable utilizar una red WiFi pública, confirmá el nombre de la misma con el responsable del establecimiento para asegurarte que es legítima.

Tené cuidado con todo lo que compartís en tus redes sociales. La información sensible como etiquetas de ubicación y de tus acompañantes puede ser la carnada ideal para los ciberdelincuentes.

Cuidate de la ingeniería social. Desconfía de cualquier mensaje inesperado o de una oferta tentadora que llegue a tus perfiles.

Activá el doble factor de autenticación siempre que puedas. Esta función brinda una capa extra de seguridad ante cualquier persona que intente loguearse en tu cuenta.

Protegete del QRishing. Desactivá la opción de abrir automáticamente los enlaces al escanear un código QR. No escanees códigos de dudosa procedencia o presentes en espacios públicos (paradas de transporte público, publicidades, plazas). Si realizarás pagos a través de códigos, verificá que la entidad, tienda o comprador sean realmente quien dicen ser. Utilizá aplicaciones de escaneo que permitan ver a qué URL dirige ese código antes de abrirlo. Desconfía cuando el QR te redirija a un sitio de descarga con archivos ejecutables.

Fuente: ***Ámbito***