Comunicado de prensa

Phishing, extorsiones y secuestros se convierten en parte de las actividades delictivas

EXPERTOS RECOMIENDAN PRECAUCIÓN AL COMPARTIR DATOS PERSONALES EN LA WEB ESTE FIN DE AÑO

El incremento en el tráfico de la información desde dispositivos móviles y computadoras durante la época festiva expone a los usuarios a ciberataques. Muchos de ellos no dimensionan las posibles afectaciones personales y familiares.

Costa Rica, 13 de diciembre de 2021

Los cibercriminales buscan víctimas expuestas, es decir, personas que comparten información sensible como: direcciones, números de teléfono, datos de cuentas bancarias, información de pagos de salarios y del aguinaldo; hasta detalles que para muchos podrían parecer inofensivos como: fotografías de la vivienda, fotografías de menores de edad y la activación de la ubicación GPS de su dispositivo electrónico. Con esto, al alcance de un "click" identifican las vulnerabilidades de la persona y combinan diversas estrategias para lograr su cometido delictivo.

Según datos del Organismo de Investigación Judicial (OIJ), se recibieron 17.457 denuncias por delitos informáticos en el 2020, un crecimiento del 24% respecto a los datos del 2019. Una de las tácticas más comunes que utilizan los ciberdelincuentes en esta época es el Phishing. Este consiste en el envío de correos electrónicos o mensajes que tienen la apariencia de proceder de fuentes de confianza, con los que solicitan información confidencial del receptor. Según Fernando Gamboa, asesor Ejecutivo y experto en seguridad de Grupo EULEN Costa Rica, "los ciberdelincuentes juegan con la emoción de los usuarios; por ejemplo, les indican que han sido ganadores de premios atractivos y les solicitan la información personal. Al mismo tiempo pueden incluso estar descargando un virus malicioso en el dispositivo para seguir filtrando información".

Las repercusiones no terminan ahí, ya que los ciberdelincuentes utilizan el contenido que encuentran en las redes sociales y demás sitios de internet para su beneficio. Las imágenes de familiares, menores de edad e inmuebles son aprovechadas para realizar otros tipos de actividades delictivas como: delitos contra la propiedad, pornografía infantil, extorsión y servicios sexuales, secuestros y paseos millonarios. Sólo durante los tres primeros meses del 2021 se registraron 124 robos en viviendas, es decir, más de un robo al día, según el OIJ.

Un control positivo

Prevenir el robo de información está al alcance de todos. En los ataques que se presentan a través de internet media el ser humano, por lo que es fundamental crear consciencia de las formas y riesgos de utilizar herramientas digitales. De acuerdo con los expertos de EULEN Seguridad Costa Rica- empresa de la multinacional española Grupo EULEN- existen recomendaciones básicas para hacer un buen uso de la información que se publica en la web:

- Primeramente, se debe definir el tipo de redes sociales en las que la persona desea inscribirse, ya sean redes de trabajo, sociales, empresariales, etcétera.
- Al abrir el perfil se tiene que elegir entre una cuenta pública o privada. Al seleccionar una cuenta privada se tiene más control de las personas que pueden ver la información publicada, por lo que hay mayor libertad a la hora de compartir contenido. Si se elige una

cuenta pública, es recomendable limitar el tipo de contenidos y datos como localización, ya que es de acceso libre para todas las personas.

- Es fundamental analizar la información que se va a publicar, de manera que esta no pueda ser utilizada para genera un daño, tanto al usuario, como a sus familiares y amigos. Al hacerse pública puede caer en manos de cualquier persona.
- En cualquier medio que se puedan recibir mensajes o solicitudes, se recomienda hacer un análisis del contenido; si es de una fuente confiable o ante la mínima sospecha optar por eliminarlo.

“Las personas pueden tener el mejor antivirus, pero es uno mismo el que entrega o protege la información. Si me piden el número de cuenta bancaria esto debería encender una alerta. Si quiero ir a pasear no es necesario divulgarlo con detalles; genere incertidumbre para que las personas no sepan el momento exacto de cada actividad”, agregó Gamboa.

En Costa Rica, EULEN Seguridad brinda servicios diversificados con estándares internacionales. Ofrece servicios de seguridad física, seguridad electrónica, y servicios mixtos o itinerantes en ambas modalidades a edificios de oficinas, centros comerciales y bancos, así como servicios de ciberseguridad a multinacionales con alta exigencia en protocolos, y a empresas logísticas con requisitos de valor añadido en control de acciones electrónicas en tiempo real.

EULEN Seguridad, lleva en Costa Rica 20 años al servicio de sus clientes con la misma vocación que al inicio de su actividad. Como empresa innovadora y flexible, se adapta a los nuevos escenarios y riesgos comprometiéndose para conseguir la excelencia en la prestación de servicios. EULEN Seguridad está especializada en vigilancia, soluciones de sistemas de seguridad, consultoría, Unidad de Inteligencia, aerovigilancia, transporte de fondos, Centro de Control de Seguridad Integral, Protección de infraestructuras críticas y seguridad integrada.

EULEN Seguridad tiene más de 45 años de trayectoria en España y es una empresa del Grupo EULEN, fundado en 1962 en Bilbao. La compañía está presente en 14 países y el volumen de ventas anuales supera los 1.600 millones de euros, con una plantilla global de más de 90 000 personas. En Costa Rica se desempeña como auxiliar de la Fuerza Pública y las policías municipales, según lo estipula la Ley de Servicios de Seguridad Privados (8395). Desde este rol estratégico EULEN Seguridad aporta las herramientas técnicas y el recurso humano experto para contribuir con los objetivos del Ministerio de Seguridad Pública.

Para más información:
Flor Monestel
flor.monestel@upgradecomunicacion.com
http://www.upgradecomunicacion.com
Tfn. +506 2506-3882 / +506 8873-2412.
Upgrade Comunicación