Seis recomendaciones para protegernos de ciberataques

La región de América Latina y el Caribe sufrió 137.000 millones de intentos de ciberataques de enero a junio de 2022, un aumento del 50 % en comparación con el mismo período del año pasado (con 91.000 millones), según datos recopilados por el laboratorio de inteligencia de amenazas, FortiGuard labs, de Fortinet

México se ubicó como el país más atacado de la región (con 85.000 millones), seguido por Brasil (con 31.500 millones) y Colombia (con 6.300 millones). Por su parte, Costa Rica sufrió 513 millones de intentos de intrusión seguido de Perú, Argentina y Brasil., lo qu representa un aumento del 104 % en comparación con el mismo periodo de 2021.

Para Pere Blay Serrano, Director del Máster en Ciberseguridad de VIU – Universidad Internacional de Valencia, es importante conocer cuáles son las dos modalidades de ciber ataques, ya que, aunque no se tenga información en la nube, se es propenso a ser víctima de hackers a través de redes Wifi o dispositivos tecnológicos *"Cuando hablamos de particulares, las estafas más comunes son aquellas destinadas al robo de dinero o de identidad, y el segundo caso suele tener también un fin económico a través de la suplantación de identidad, ya sea para obtener dinero de la víctima directamente, o bien para usar su identidad y engañar a terceros".*

Phishing

En este sentido, el phishing (intento de robo de usuario y contraseñas, por medio de e-mails o llamadas), y el smishing (a través de SMS) son las dos técnicas más habituales de acuerdo con el experto de VIU.

Sin embargo, destaca que el ciberdelincuente puede instalar algún malware de forma involuntaria a través de links o imágenes compartidas por redes sociales, en nuestros dispositivos (PCs, tablets, o smartphones). De manera que el hacker, puede estar espiando nuestra actividad, capturando usuarios y contraseñas, robando fotos o documentos, etc.

Dichas técnicas se incrementaron en el año 2022 con una nueva modalidad que se potenció con la guerra en Ucrania. Según el Informe de Defensa Digital anual de Microsoft, elaborado en base a información de ciberseguridad recabada entre julio de 2021 y junio de 2022 en todo el mundo, se observó un alarmante incremento de correos electrónicos que se hacían pasar por organizaciones que solicitaban donaciones de criptomonedas en Bitcoin y Ethereum para apoyar a los ciudadanos ucranianos.

¿Qué hacer frente a ciberataques?

En busca de prevenir está serie de **ciberataques** que, con los años, se vuelven más masivos y preocupantes, Blay Serrano, brinda las siguientes recomendaciones:

1. No abrir links sin revisarlos antes, tampoco compartirlos, aunque los envíe un conocido. Comprobar si tienen caracteres extraños, o si se parece un link de un sitio conocido, pero cambia un poco. También existen plataformas en la red para contrastar si un link es malicioso.

2. No hacer caso de mensajes por SMS, si son de paquetería, sobre todo si no estamos esperando recibir nada. En caso de que, si esperamos una entrega mejor contrastar llamando a la empresa encargada del reparto.

3. Nunca hacer gestiones con el banco o administración por SMS, o si nos llaman por teléfono, mejor finalizar la llamada y contactar posteriormente con nuestro banco o con la administración por los medios oficiales, tampoco caer en la compra de ofertas espectaculares si no estamos seguros que vienen de un portal de compras seguro.

4. No reenviar mensajes ni compartir contenido que pueda ser fake (en muchas ocasiones generan confusión que facilita la labor de los ciberdelincuentes).

5. Nunca compartir documentos, imágenes o videos que sean de contenido privado o que pueda comprometer nuestra integridad personal. Si en las imágenes o videos que compartimos salen terceros, preguntar antes si les parece bien que el contenido sea compartido.

6. Usar contraseñas complejas y/o utilizar gestores de contraseñas seguros. Lo mismo para medios de pago que

contengan información de nuestras tarjetas bancarias. Utilizar únicamente servicios de este tipo con seguridad contrastada y, en todo caso, activar siempre doble verificación por llamada o SMS.

Finalmente, es importante recalcar que a nivel global existe un nivel de escasez de profesionales en el ámbito de la ciberseguridad y ciberataques. De acuerdo con el informe de Defensa Digital de Microsoft. Y en este sentido es fundamental que cada vez más personas se involucren en el aprendizaje de estas problemáticas que día a día se incrementan logrando daños tanto el sector público como en el privado.