

Tips para protegernos de ataques cibernéticos

En lo que va del año los ataques cibernéticos han aumentado un 24% en Latinoamérica. Según un estudio realizado por el gigante ruso de la ciberseguridad, Kaspersky; los países más atacados son Brasil, con más de 5 millones de intentos de ataque este año, seguido por Colombia con 1,8 millones, México con 1,7 millones, Chile 1 millón y Perú 507 millones.

El informe también destaca que Costa Rica con un 378%, Venezuela 113% y Argentina 91% son los países con mayor crecimiento en ataques de RDP en comparación al año pasado.

Para Pere Blay Serrano, Director del Máster en Ciberseguridad de VIU – Universidad Internacional de Valencia, es importante conocer todos los tipos de ataques, ya que, aunque no se tenga información en la nube, se es propenso a ser víctima de los hackers a través de redes Wifi o dispositivos tecnológicos.

“Hoy en día una formación básica en ciberseguridad es imprescindible y debería incorporarse sin retraso como parte de la educación en escuelas e institutos», acotó.

«Con nuestros dispositivos móviles, tablets, portátiles y PC estamos continuamente conectados a la red y eso nos hace vulnerables a todo tipo de amenazas. Desde intentos de phishing, conseguir datos de acceso a cuentas bancarias, números y pin de tarjetas de crédito, hasta robo de datos personales o violaciones de nuestra privacidad”, agregó.

Algunos de los peligros más comunes a los que están expuestas las personas son:

Suplantación de identidad

Para tener control sobre la cuenta bancaria, la tarjeta o incluso la línea de teléfono. Casi siempre con fines lucrativos, es decir, conseguir acceso al dinero o solicitar rescate o extorsión.

Timos

Se solicita dinero por algún servicio falso, como supuestos paquetes que se esperan recibir, o devoluciones inesperadas de entregas que se realizaron hace meses o promesas de recuperar mucho más dinero si se hace una determinada inversión.

Relaciones románticas

Supuestas personas que muestran algún tipo de afecto y comienzan a jugar con los sentimientos de la víctima, aprovechándose para pedir ayuda económica, con el pretexto de tener interés por viajar y conocer a la persona.

Prevención

De igual forma, el director del máster en ciberseguridad de VIU recomienda los siguientes tips para evitar cualquier modalidad de ciberataque:

- 1.- No abrir links sospechosos que alerten sobre irregularidades bancarias o entregas de paquetes que no se pidieron.
- 2.- Usar antivirus y actualizar siempre que sea necesario nuestros smartphones y tablets. La mayoría de actualizaciones incluyen mejoras en la seguridad.
- 3.- Usar contraseñas que incluyan números y símbolos.
- 4.- No compartir datos personales con nadie que no sea de confianza.
- 5.- No reenviar fake news ni avisos o noticias que no se hayan corroborado.

Finalmente, Blay Serrano recalca que los gobiernos también son blanco fuerte de los ciber terroristas, ya que la información que buscan los ayuda notablemente en sus objetivos

“El ciberterrorismo es una amenaza muy presente y real. Todos los cuerpos de seguridad del estado cuentan con secciones dedicadas al ciberespacio para vigilar y detectar posibles amenazas. Pero el ciberterrorismo no se limita a ataques por la red. La red puede servir para robar y compartir información sensible que sea de interés para grupos terroristas y que les

ayude a fijar sus objetivos, ya que pueden causar daños muy costosos de reparar y que afecten a mucha gente, incluso poner vidas en peligro en el caso, por ejemplo, de verse afectados hospitales o servicios importantes para nuestra salud”.