5 recomendaciones para fortalecer la ciberseguridad en 2022

Es habitual usar contraseñas comunes, conectarse a redes de internet públicas o abrir correos que parecen proceder de instituciones confiables (como bancos, tiendas departamentales, entre otros), pero que en realidad pretenden robar información del usuario, esto es denominado phishing.

Según ESET, durante el 2020 se registraron solo en Latinoamérica el doble de correos de phishing que en 2019; y en lo que va de 2021 la cantidad de detecciones volvió a duplicarse con respecto al 2020. Además, en 2021 van detectados más de 2.1 millones de archivos únicos relacionados con este tipo de campañas, 31% más que en 2022 y 132% más que en 2019.

La buena noticia es que el inicio de Año Nuevo es una gran oportunidad para tomar acciones sobre esto y es así como los expertos de ESET mencionan otros de los cibercrímenes más populares para evitar que caigas en algunos de ellos:

- Malware: Una de las formas pioneras de la ciberdelincuencia es el malware, el cual de acuerdo a su funcionalidad podría desde infectar sistemas informáticos, destruir archivos, o hasta incluso cambiar el funcionamiento en general de los dispositivos y asaltar sistemas. Cabe mencionar que dentro del malware está el ransomware, programa que bloquea archivos hasta que se pague un rescate por ellos.

- Robo de identidad: Consiste en el uso de la información de una persona sin su consentimiento. Los criminales extraen la información para hacerse pasar por otros y actuar bajo este nombre con la finalidad de robar cuentas bancarias, pedir préstamos o hacer actos ilícitos bajo otra identidad.

- Cryptojacking: Consiste en entrar a un dispositivo y minar criptomonedas del dispositivo del usuario sin su conocimiento. En su mayoría, los criptomineros utilizan Javacript para llevar a cabo este delito, todo por medio de un sitio web infectado.

- Ciberextorsión: Una de las maneras más comunes de hacer ciberextorsiones es por medio del ransomware, el cual se encarga de infectar un equipo con un malware que cifra todos los archivos. Todo con el propósito de pedir un rescate por esos datos.

- Ataques de fuerza bruta: Según la telemetría de ESET, desde abril de este año, se notó un aumento exponencial en la detección de ataques de fuerza bruta a clientes RDP, además cuenta con un registro de crecimiento del 32% en Latinoamérica durante el 2021.

Bajo este panorama, uno de tus propósitos más importantes de Año Nuevo debe ser aprender más sobre ciberseguridad y estar mejor preparados para lidiar con las distintas amenazas en Internet. Como primer paso se puede tomar conciencia de la importancia que tienen nuestros dispositivos hoy en día, pues puede quedar expuesta nuestra información ante ciberamenazas que llegan a

perjudicar la privacidad digital o llegar hasta un caso de extorsión. Por esto, expertos de ESET te comparten 5 recomendaciones de oro para que empieces a cuidar de tu ciberseguridad:

- Asegúrate de que ninguna de tus contraseñas aparezca en la lista de los criminales, también conocida como la lista de las claves más populares. Las combinaciones menos complejas pueden ser fáciles de recordar, pero son igual de fáciles de descifrar.

- Utiliza contraseñas fuertes, o mejor aún: emplea frases. Cuanto más larga sea, más tiempo los llevará adivinar a los cibercriminales tus claves de acceso.

- Reutilizar tus contraseñas solo afectará tu seguridad y privacidad en Internet. Los cibercriminales tienen más de una herramienta para irrumpir en tus cuentas, una táctica es el ataque de credential stiffing, por eso no es recomendable reusar este tipo de información.

- Usa un administrador de contraseñas confiables para mantener seguras todas tus claves mientras recuerdas solo una. Con este método será posible almacenar de forma segura tus datos de inicio de sesión.

- Comprueba periódicamente que ninguna de tus cuentas haya sufrido un ataque. Es importante verificar regularmente si las credenciales han sido parte de una brecha, esto es posible por medio de sitios web que te mostrará una lista de servicios asociados a tu cuenta de correo electrónico que te mostrará si tu cuenta sufrió una amenaza o si algún dato fue comprometido.