Advierten por el crecimiento de ciberataques y estafas en compras electrónicas

28/03/2022

Especialistas advierten el crecimiento de ciberataques y estafas registrados en los últimos años en Argentina en las compras electrónicas y pronostican que en 2022 también impactará en nuevas industrias como el mercado de las criptomonedas.De acuerdo a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) en Argentina se registró sólo en 2020 “una suba del 70% de los delitos informáticos, lo que equivale a todos los delitos cometidos en los 5 años anteriores a la pandemia».

A modo de ejemplo señalaron que «las estafas con compras electrónicas crecieron un 106% y las denuncias de robo de identidad un 700%.

«Sabemos que en 2022 esta tendencia seguirá en alza, e impactará en nuevas industrias como es el mercado de las criptomonedas”, dijo a Télam el especialista en ciberseguridad

de la empresa especializada VU, Pablo Lima.

“A nivel mundial, la rápida digitalización de actividades trajo como consecuencia natural un aumento en las vulnerabilidades”, agregó Lima.

“Según el último reporte de la Dirección Nacional de Ciberseguridad en 2021 se registró un aumento interanual de incidentes informáticos del 261%, siendo los más importantes los casos reportados relacionados a phishing, modificación no autorizada de la información y spam”, detalló el especialista.

En tanto, “el fraude, con 331 casos, representa el 56% del total de incidentes reportados, lo que lo convierte en el delito informático que más se registró durante el período mencionado”.

De acuerdo a Lima, a nivel global “se estima que las pérdidas económicas por ciberataques pueden alcanzar un trillón de dólares, con un promedio de US$ 3.9 millones por cada brecha de seguridad”.

Ante este cuadro de situación, los especialistas recomiendan actualizar programas y sistemas operativos para proteger tanto a los usuarios finales como a las organizaciones para salvaguardar sus activos digitales; utilizar contraseñas robustas; implementar certificados de seguridad, y activar factores de autenticación, lo que eleva los niveles de seguridad, permitiendo limitar en un 100% los casos de phishing.

Lima advirtió además, que existe otra modalidad delictiva, el ransomware, que también se encuentra en alza “gracias al anonimato que ofrece debido a su tecnología”.

«Se trata de un tipo de virus que encripta información, secuestra esos datos y bloquea accesos a los sistemas, y su finalidad es extorsionar, pidiendo la devolución de esta información sensible, a cambio de altas sumas de dinero, o

incluso criptomonedas”, explicó.

“En Argentina, si bien contamos con un marco regulatorio y un sistema de políticas públicas significativamente consolidados, queda mucho por hacer”, señaló Lima, tras lo cual enfatizó que “sabemos que tanto los ataques como la digitalización irán en aumento, y eso debe estar acompañado de programas que integren tanto al sector público como el privado».

«El desafío es importante para todos los sectores: los responsables de la ciberseguridad y de TI deben hacer frente a nuevas tácticas, técnicas y procedimientos que amenazan a la continuidad de los negocios, pero también es necesario invertir tiempo en informar y capacitar a los usuarios, para que tengan mejores herramientas para tomar sus decisiones”, agregó.

El especialista dijo que “la fuga, robo y pérdida de información confidencial, pueden provocar crisis de reputación en una marca, incumplimientos legales y afrontamiento de multas, que en muchos países con regulaciones estrictas pueden llegar hasta el 4% de la facturación anual de una empresa”.

“Según nuestros últimos reportes, las empresas de la región están aumentando la inversión en ciberseguridad desde hace años, no solo para evitar este tipo de ataques, porque una brecha de seguridad puede poner en juego otros factores que son tanto o más perjudiciales para la organización, como lo es el impacto a la reputación y la pérdida de confianza”, concluyó.