Estafas, «ransomware», fuga de datos: estos han sido los grandes hitos en ciberseguridad de 2019

Incibe ha recogido los mayores riesgos a del año para usuarios y empresas en internet

El Instituto Nacional de Ciberseguridad (INCIBE) ha recopilado los 10 hitos más destacados en materia de ciberseguridad de 2019, entre ellos casos de «phishing», retos virales y los juguetes conectados. El año comenzó con una de las mayores filtraciones de correos electrónicos hasta la fecha, denominada **Collection #1.** INCIBE advirtió en enero a los usuarios sobre esta brecha de seguridad, que **expuso hasta 773 millones de cuentas de todo el mundo.**

A diferencia de otras filtraciones, Collection #1 compilaba datos obtenidos a través de diferentes páginas web y servicios, según señaló en un comunicado. La mayoría de usuarios se vieron afectados debido a la reutilización de contraseñas para diferentes servicios, lo que supuso un **enorme riesgo para su privacidad.**

«Phishing» y otras estafas

A lo largo de 2019 muchas organizaciones y usuarios han sido víctimas de ataques de «phishing». En septiembre, INCIBE detectó una **campaña maliciosa de correos electrónicos fraudulentos** que pretendía extorsionar a los destinatarios con un presunto vídeo de contenido sexual. Concretamente, el ciberdelincuente **amenazaba con enviar un supuesto vídeo a los contactos de la víctima** en 72 horas si esta no realizaba un pago de 2.000 euros en bitcoins.

Los correos electrónicos se enviaban con el asunto **«¡Esta es mi última advertencia!»** y para contar con una mayor credibilidad, en el mensaje **se informaba a la víctima sobre cómo se habría infectado su equipo.**

Los **anuncios fraudulentos** con imágenes de personas de reconocido prestigio y reputación también aumentaron a lo largo de 2019. Este tipo de anuncios, que aparecen en diversos medios de comunicación y plataformas digitales, tenían el objetivo de **ganarse la confianza de los usuarios** para tratar de convencerles para que ingresen dinero en una cuenta bancaria.

Esta técnica ha ido evolucionando y se ha vuelto más sofisticada, como demuestran los fraudes de Recursos Humanos y del CEO que tuvieron mucho impacto en España y otros países.

INCIBE **detectó en julio una importante cantidad de timos** que suplantaban la identidad de trabajadores de una empresa para ponerse en contacto con el departamento de Recursos Humanos y solicitar un cambio de cuenta para recibir la nómina.

Retos virales y bulos

Este año también han destacado los retos virales, como **«la ballena azul»** que **alentaba a los jóvenes a suicidarse**. Sin embargo, el más peligroso de 2019 ha sido **«Momo»** Aunque surgió por primera vez en julio de 2018, la fotografía de la escultura con una apariencia terrorífica volvió en 2019 con un nuevo argumento que **incitaba a la autolesión**. Este reto causó una gran preocupación entre los padres debido a la falta de conciencia crítica de los menores.

Para mitigar el impacto de esta amenaza, INCIBE publicó a través de Internet Segura for Kids (IS4K) un artículo en el que ofrece diferentes recomendaciones para los padres, como trabajar la educación digital o la mediación parental.

En cuanto a las **cadenas virales**, que se han ido adaptando al formato de cada red social para llegar a más personas, INCIBE publicó otro artículo haciendo hincapié en la importancia de la **alfabetización mediática como contrapartida a los bulos.**

De esta forma, el Instituto pretendía ayudar a que los menores aprendan de forma sencilla a detectar **«fake news»** -noticias falsas y desinformación- y tener un pensamiento crítico a la hora de compartir informaciones.

Videojuegos

En 2019, INCIBE ha recalcado la importancia del **uso responsable de los videojuegos** en niños y adolescentes, ya que muchos hogares cuentan con videoconsolas, muchas de las cuales incluyen la conexión a Internet.

Sin embargo, muchos usuarios desconocen los riesgos a los que pueden estar expuestos. Por ello, INCIBE ha fomentado entre los padres el **juego en positivo**, acompañando al menor y dialogando con él para **enseñarle a gestionar peticiones de amistad** de desconocidos, situaciones conflictivas en partidas e incluso mensajes inadecuados.

Asimismo, publicó junto a la Asociación Española de Fabricantes de Juguetes (AEFJ) una guía para garantizar la fabricación segura y responsable de los **juguetes conectados**, también conocidos como «Smart Toys». El objetivo de esta guía es **garantizar un nivel adecuado de seguridad en el diseño y la fabricación de los juguetes** que cuentan con conexión a Internet.

Entre las principales medidas de protección que los fabricantes deben incluir desde la creación de un juguete, hasta que deja de prestar soporte, **la guía incluye la realización de evaluaciones de privacidad** y la implementación de estándares de seguridad.

Otro de los hitos en seguridad más destacados de 2019 ha sido el **«sharenting»** definida como compartir en las redes sociales **fotografías de hijos menores**. Actualmente se trata de un práctica habitual para algunos padres, pero no tienen en cuenta el **riesgo que puede suponer para sus hijos.**

Según INCIBE, el principal problema reside en la **pérdida de privacidad de los menores**, lo que implica varios riesgos como el uso malintencionado de las fotografías por parte de desconocidos o la suplantación de identidad.

«Botnets» y «ransomware»

INCIBE informó a principios de noviembre de que estaba investigando un ciberataque a través de **«ransomware»** un tipo de virus que **encripta los archivos y exige el pago de rescates** para recuperarlos, que afectaba a varias empresas españolas.

La cadena SER confirmó que fue una de las empresas afectadas y afirmó haber sufrido una «afectación grave y generalizada de todos sus sistemas informáticos» a causa del virus, como recoge el Instituto Nacional de Ciberseguridad.

Meses antes, el Instituto publicó un aviso sobre una **vulnerabilidad en el escritorio remoto de Windows** que podría ser aprovechada por ciberdelincuentes para propagarse de un equipo vulnerable a otro.

INCIBE también detectó este año una **campaña de envío de correos electrónicos fraudulentos** que pretendían que la víctima descargara un documento malicioso para que el equipo pasara a formar parte de la «botnet» Emotet .

Para que las empresas afectadas se recuperaran de este tipo de redes zombie, INCIBE realizó importantes cambios en su Servicio Antibotnet y **elaboró varios contenidos en los que explicaba cómo saber si una organización forma parte de una botnet** y cómo protegerse de ellas.

Compras «online»

Cada vez son más usuarios los que deciden realizar sus compras de forma «online» debido a la comodidad y el ahorro de tiempo, pero esta modalidad también tiene algunos riesgos de seguridad.

La compra segura a través de internet ha sido uno de los asuntos que más ha preocupado a los usuarios este año. En junio, INCIBE publicó una campaña sobre compras online seguras advirtiendo de **plataformas falsas, perfiles falsos de vendedor y métodos de pago poco fiables.**

Tras esta campaña se identificaron en nuestro país **más de 30 tiendas online fraudulentas** que eran gestionadas por el mayor ciberestafador de España hasta entonces.

La Guardia Civil detuvo a un joven de 23 años que poseía unos ingresos generados por estos fraudes que podían alcanzar hasta 300.000 euros mensuales.

Fuente: ABC