
Sean bienvenidos una vez más a Código Seguro. Los medios de comunicación son una herramienta esencial para la sociedad y un vector considerable de contenidos anómalos. Muchos ciberdelincuentes diseñan diariamente mensajes de estafa dañinos que se envían a millones de personas en todo el mundo aprovechando los avances tecnológicos. Los servicios de correo electrónico ofrecen una forma gratuita, posiblemente anónima y rápida, de propagar las estafas a través de Internet.

El correo spam, también conocido como correo basura, ha sido una preocupación en internet desde sus inicios. Aunque el término “spam” se popularizó en los años 80, la práctica de enviar mensajes no solicitados data de 1864 con el uso del telégrafo para enviar ofertas de negocios dudosas. Ya en la década de 1970, personas malintencionadas en la lista de correo de ARPANET comenzaron a enviar mensajes no deseados en masa. Pero fue en 1994 cuando dos abogados de Phoenix (Laurence Canter y Martha Siegel) enviaron un mensaje publicitario a través de USENET, lo que realmente inmortalizó el uso del término “spam” para referirse al correo no deseado. A pesar de las críticas, la campaña fue un éxito financiero, lo que llevó a la pareja a dedicarse profesionalmente al spam y hasta publicaron un libro de su autoría sobre cómo aumentar los ingresos personales a través de internet.

El spam representa hoy en día un porcentaje significativo de todo el

correo electrónico y es una amenaza para la seguridad en la red. Las técnicas de phishing y otros métodos fraudulentos a menudo se distribuyen a través de correos spam, lo que hace que la lucha contra estos correos no deseados sea una cuestión de gran importancia. Sin dudas, representa uno de los problemas más grandes de la comunicación electrónica actual. Estimaciones bastante cercanas a la realidad nos dicen que aproximadamente el 50% de todos los correos electrónicos podrían ser catalogados de esta forma. Este término se refiere a cualquier tipo de comunicación no solicitada que se envía de forma masiva, ya sea por correo electrónico, mensajes instantáneos, SMS, redes sociales o incluso mensajes de voz.

Tradicionalmente, estos se han considerado solo correos molestos y no solicitados que contienen publicidad, pero cada vez incluyen más estafas, programas maliciosos o técnicas de ingeniería social como el phishing. Las consecuencias para los usuarios y las organizaciones en general son múltiples y pueden ser bastante perjudiciales:

Pérdida de tiempo: Los usuarios y empleados de empresas pueden perder horas cada mes eliminando estos molestos mensajes, que se van acumulando poco a poco, lo que reduce la productividad y el tiempo de trabajo efectivo.
Desmotivación: La necesidad de eliminar manualmente el spam puede causar frustración y emociones negativas en los usuarios.
Sobrecarga en las comunicaciones: Debido a que puede bloquear los canales de comunicación y generar tráfico innecesario, lo que resulta en costos adicionales tanto para los proveedores de servicios como para los usuarios o empresas.
Criminalización del spam: Estos simplemente han ido creciendo en el tiempo. De ser una simple molestia publicitaria, se han convertido en una herramienta para realizar otros tipos de ataques como la infección de sistemas informáticos y el robo de información confidencial.
Consumo de recursos de red: El spam consume ancho de banda y espacio de almacenamiento, dejando menos recursos disponibles para actividades productivas y obligando a invertir en hardware y software para su transmisión, análisis y filtrado.
Riesgo de perder correos importantes: Al tener que lidiar con grandes cantidades de spam, existe el riesgo de eliminar accidentalmente correos electrónicos importantes.
Pérdidas económicas: Además de los costos operativos, puede causar daños en los sistemas y robo de información financiera, resultando en pérdidas económicas directas para las empresas.
Daños de reputación: Si una cuenta de correo o página web es hackeada para enviar spam, esto puede dañar la reputación de la empresa o individuo afectado. Estas cuentas pueden ser dadas de alta en listas negras internacionales de las cuales en la concreta cuesta mucho trabajo salir de ellas.

Para garantizar la seguridad y la integridad de los usuarios, disímiles organizaciones e investigadores han tratado y seguirán tratando de desarrollar filtros robustos para la detección del correo basura. Recientemente, la mayoría de estos filtros de spam basados en algoritmos de aprendizaje automático (inteligencia artificial) publicados en revistas académicas presentan un rendimiento muy elevado, sin embargo, los usuarios se mantienen denunciando un número creciente de fraudes y ataques a través de correos electrónicos basura. En esta área del conocimiento se plantean dos retos principales:

Es un entorno muy dinámico, propenso al problema del cambio de conjunto de datos.
Adolece de la presencia de una figura adversaria, es decir, el spammer.

Estos últimos –es decir, cualquier persona u organización que envíe correos electrónicos no deseados– obtienen un beneficio utilizando estafas incluidas en los correos electrónicos y, de este modo, tratan de mantenerse invisibles para los filtros desarrollados. Para lograr su propósito, aplican continuamente nuevas estrategias para eludir los mecanismos existentes de detección, aprovechando los puntos débiles. Actualmente, utilizan técnicas de manipulación textual, conocidas como envenenamiento de texto y palabras ofuscadas, en todo el cuerpo de los correos electrónicos o en determinadas palabras dentro de él, por ejemplo, errores ortográficos o adición de palabras aleatorias o ilegítimas a un mensaje de spam. De esta forma, los spammers pueden ser considerados como la figura adversaria en este campo. Varios autores de la literatura científica, desde hace más de diez años, advertían ya de que el correo electrónico no deseado no estaba muriendo, sino volviéndose más elegante y cada vez más sofisticado.

Lo que conlleva a los especialistas en ciberseguridad a desarrollar soluciones informáticas centradas especialmente en los problemas que plantea este entorno en constante cambio, a diferencia de los principales análisis clásicos existentes. Además, para protegernos del spam, es recomendable no publicar tu dirección de correo en sitios web públicos y manejarla con precaución, algo que realmente los usuarios realizan con frecuencia, olvidando la percepción del riesgo al interactuar con las diferentes plataformas electrónicas y las redes sociales mundiales. El proceso de registro de los usuarios en estas aplicaciones de internet siempre comienza con la inserción de una dirección electrónica. Recomendamos que para estos casos pudieras crear una dirección de correo secundaria, no relacionada la cuenta principal que puedas utilizar para suscripciones y boletines en dichos servicios.

Además, por lo general, los servidores de correo electrónico existentes en Internet ofrecen herramientas para marcar correos como spam y mejorar la eficacia del filtro de correos no deseados que viene por defecto. En el ámbito legal también se deben disponer de mecanismos que regulen todo esto. En nuestro país, aunque no hay una ley específica que se refiera exclusivamente al spam, el Decreto Ley 35/2021 establece regulaciones generales para el uso de las tecnologías de la información y las comunicaciones, incluyendo aspectos de ciberseguridad. No obstante, el Decreto No. 360/2019 del Consejo de Ministros, a través de su artículo 49, demanda total prohibición sobre el envío de mensajes no deseados de forma masiva.

A pesar de los esfuerzos regulatorios y tecnológicos para combatirlo, el spam persiste, adaptándose continuamente a las medidas de protección. Por lo tanto, es esencial que los usuarios estén informados y equipados con las herramientas y prácticas necesarias para minimizar su exposición al spam y sus efectos nocivos. En última instancia, la lucha contra el spam es una responsabilidad compartida entre legisladores, proveedores de servicios de internet, organizaciones y usuarios finales. Solo a través de un enfoque colaborativo y la implementación de estrategias integrales se podrá mitigar este problema en el ámbito de la comunicación digital. Por hoy nos despedimos hasta la próxima semana.

Cubadebate.