Vol.7 No.4 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.4.2023.515-531

Vulnerability analysis through massive spam in ISPs clients in the Huaquillas canton.

Análisis de vulnerabilidades a través de spam masivos en clientes de ISPs en el cantón Huaquillas.

Autores:

Pulla-Tumbaco, Jonathan Manuel
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

jonathan.pulla.02@est.ucacue.edu.ec

https://orcid.org/0009-0006-9461-3837

Cuenca-Tapia, Juan Pablo
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

jcuenca@ucacue.edu.ec

https://orcid.org/0000-0001-5982-634X

Ortega-Castro, Juan Carlos
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

jcortegac@ucacue.edu.ec

https://orcid.org/0000-0001-6496-4325

Fechas de recepción: 02-SEP-2023 aceptación: 02-OCT-2023 publicación: 15-DIC-2023

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Problema: el spam es un gran problema para los ISP, ya que los spammers utilizan técnicas avanzadas para enviar correo no deseado de forma eficiente, sobrecargando los sistemas de correo y generando problemas de seguridad para los usuarios. Objetivo: Analizar las técnicas de spam empleadas en los ataques cibernéticos mediante el envío excesivo de spam a las cuentas de correo electrónico de los clientes de los ISPs del cantón Huaquillas haciendo uso de herramientas basadas en Kali Linux con el fin de implementar medidas de control efectivas para prevenir este tipo de ataques. Metodología: Se utilizó una metodología mixta en la investigación, esto permitió recopilar datos cuantitativos sobre la frecuencia y volumen de spam, mientras se obtenía una comprensión cualitativa de la experiencia y percepción de los clientes de ISPs en relación con estas vulnerabilidades. Esta combinación de enfoques fue utilizada para obtener una visión más completa y holística del problema. Resultados: En el contexto del primer escenario, se pudo identificar que el 97.56% de los participantes amablemente compartió su dirección de correo electrónico, mientras que aproximadamente el 2.44% optó por no proporcionarla. Este análisis revela una proporción significativa de correos electrónicos comprometidos, lo cual plantea una posible vulnerabilidad en materia de seguridad. Estos resultados subrayan la imperante necesidad de implementar medidas concretas para salvaguardar de manera efectiva la información personal y prevenir la exposición a posibles estafas.

Palabras clave: isp, spam, setoolkit, vulnerabilidades, software, kali linux.

Abstract

Problem: Spam is a major issue for ISPs as spammers employ advanced techniques to efficiently send unsolicited emails, overloading email systems and posing security risks to users.

Objective: To analyze spam techniques used in cyberattacks through excessive spamming of email accounts belonging to ISPs' customers in Huaquillas Canton, using Kali Linux-based tools, in order to implement effective control measures to prevent such attacks.

Methodology: A mixed methodology was employed in this research, enabling the collection of quantitative data on spam frequency and volume, while also gaining qualitative insights into the experiences and perceptions of ISPs' customers regarding these vulnerabilities. This combination of approaches was utilized to achieve a comprehensive and holistic understanding of the problem.

Results: In the context of the first scenario, it was identified that 97.56% of the participants willingly shared their email addresses, while approximately 2.44% chose not to provide them. This analysis reveals a significant proportion of compromised emails, indicating a potential security vulnerability. These findings underscore the urgent need to implement concrete measures to effectively safeguard personal information and mitigate the risk of falling victim to scams.

Keywords: isp, spam, setoolkit, vulnerabilidades, software, kali linux.

Introducción

El envío masivo de correo no deseado o spam es un problema importante para los clientes de los proveedores de servicios de Internet (ISPs). Esto se debe a que los spammers a menudo utilizan técnicas avanzadas para enviar spam a una gran cantidad de direcciones de correo electrónico de manera eficiente, lo que puede causar una sobrecarga en los sistemas de correo electrónico y generar problemas de seguridad para los usuarios. (International IT, 2022).

En el ámbito local, el envío masivo de correo no deseado o spam también se convierte en un problema importante para los clientes de los proveedores de servicios de Internet (ISPs). Como en cualquier otra región, los spammers utilizan técnicas avanzadas para enviar grandes volúmenes de spam de manera eficiente. Sin embargo, en el contexto específico de Huaquillas, este problema puede tener repercusiones adicionales.

En Ecuador se realizó un estudio Epidemiológico en el año 2010, en el cual se encontró una prevalencia de caries dental en niños de 6 años de un 79,9%, en niños de 12 años de un 60,8% y en niños de 15 años de un 71,5%. Por otra parte, la existencia de inconsistencias y vacíos de la normativa, (Castañeda & Sotelo, 2023) han dado origen a diversos problemas y que la implementación de estrategias que buscan reducir algunos indicadores no ha recibido seguimiento y que el modelo de atención pública integral de salud aún no se cumple totalmente.

Además de los inconvenientes operativos, el spam también representa un riesgo de seguridad significativo para los usuarios locales en Huaquillas. Los spammers pueden aprovecharse de las técnicas de phishing para engañar a los destinatarios y obtener información confidencial, como contraseñas o datos bancarios. Esto puede resultar en un robo de identidad, fraude financiero u otros delitos cibernéticos que pueden tener un impacto económico y emocional en los usuarios.

Material y métodos

Descripción de la Encuesta:

La encuesta utilizada en esta investigación tuvo como objetivo principal ser la brecha por la cual se obtendrían los correos electrónicos de las personas que respondieron. Fue diseñada para obtener información de una población específica, que consistió en los clientes de los distintos ISP del cantón. La encuesta constaba de un total de 14 preguntas, cuidadosamente diseñadas para abordar los aspectos clave del tema de investigación. Su diseño se basó solo en preguntas de selección múltiple.

Setoolkit:

Setoolkit desempeñó un papel fundamental en esta investigación, dado que nos proporcionó herramientas y recursos para llevar a cabo una parte crucial del estudio. Se utilizó con el propósito de enviar correos masivos a las direcciones de correo electrónico obtenidos de la encuesta. En particular, se configuró Setoolkit de acuerdo con las necesidades específicas de la investigación. Se utilizaron funciones específicas, como Mass Mailer Atack para llevar a cabo el envío masivo de correos.

Planes y acciones técnicas para fortalecer la seguridad en línea y mitigar el impacto del correo no deseado (spam).

Es vital implementar un plan efectivo para prevenir y combatir el spam masivo y proteger la confidencialidad de los usuarios. El plan debe incluir medidas técnicas y acciones educativas para fortalecer la ciberseguridad y promover prácticas seguras entre los clientes de los proveedores de servicios de Internet en Huaquillas. Se han considerado las mejores prácticas de la norma ISO 27001, reconocida internacionalmente en seguridad de la información. A continuación, se presentarán alternativas para abordar este problema:

1. **Filtrado de correos electrónicos basado en reglas:**
   - Se recomienda implementar un sistema de filtrado de correos electrónicos basado en reglas predefinidas para bloquear mensajes de spam. Esta práctica cumple con las recomendaciones de la norma ISO 27001 sobre seguridad de la información.

2. **Autenticación de remitentes mediante SPF y DKIM:**
   - El uso de SPF y DKIM ayuda a verificar la autenticidad de los remitentes de correos electrónicos, cumpliendo así con las recomendaciones de la norma ISO 27001 para la seguridad de la información y la protección de datos.

3. **Soluciones de seguridad de red:**
    - Se recomienda utilizar soluciones de seguridad de red, como firewalls e IDS/IPS, para detectar y bloquear actividades de spam. Estas medidas cumplen con las pautas de la norma ISO 27001 para proteger la integridad y disponibilidad de la información.

4. **Educación y concientización de los usuarios:**
    - Implementar programas educativos para clientes de ISPs en Huaquillas para prevenir riesgos de spam, phishing y estafas.
    - Proporcionar materiales educativos, guías de seguridad y talleres interactivos para promover la seguridad en línea y fomentar comportamientos seguros en el uso del correo electrónico.

5. **Actualizaciones y parches de seguridad:**
    - Mantener actualizados los sistemas operativos, aplicaciones y software de seguridad en los equipos y servidores de los ISPs para asegurar la protección contra las últimas vulnerabilidades conocidas y ataques de spam.

6. **Evaluación y mejora continua:**
    - Realizar evaluaciones periódicas de la efectividad de las medidas de mitigación implementadas y realizar ajustes y mejoras según sea necesario.
    - Mantenerse al tanto de las nuevas tendencias y técnicas de spam masivo para adaptar el plan de mitigación y mantener una defensa sólida contra las amenazas emergentes.

Metodología

Se adaptó una metodología mixta donde se combinó enfoques cualitativos y cuantitativos. Esta metodología permitió recopilar datos cuantitativos sobre la frecuencia y volumen de spam masivo, así como obtener una comprensión cualitativa de la experiencia y percepción de los clientes de los ISPs en relación con estas vulnerabilidades. A continuación, se proporciona una descripción detallada de la metodología utilizada para abordar el tema mencionado:

1. **Fase exploratoria:**
    - Se realizó una revisión de literatura sobre spam masivo, vulnerabilidades de seguridad y medidas de protección en el contexto de los clientes de ISPs.

- Establecer los objetivos de la investigación y las preguntas de investigación específicas.

2. **Selección de la muestra:**
   - Se determinó la población objetivo, en este caso, los clientes de diferentes ISPs en el cantón Huaquillas.
   - Se utilizó técnicas de muestreo adecuadas para seleccionar una muestra representativa de la población objetivo.

3. **Recopilación de datos cuantitativos:**
   - Se decidió hacer uso de la herramienta Google Forms para crear la encuesta, la cual se presentó de manera presencial ante los gerentes de los diversos ISPs del cantón. Esto se hizo con el propósito de contar con su colaboración en la difusión de la misma.
   - Se realizaron los análisis de los registros de correo electrónico obtenidos de los clientes de los ISPs.

4. **Recopilación de datos cualitativos:**
   - Se exploró temas como las medidas de seguridad percibidas, los desafíos para lidiar con el spam y las posibles repercusiones en la seguridad de sus sistemas.

5. **Fase práctica:**
   - Entre los datos recopilados, se incluyeron las direcciones de correo electrónico, ya que este fue el medio principal utilizado para el envío masivo de spam. Para llevar a cabo esta tarea.

   - Se empleó la herramienta Setoolkit, en particular, se utilizó la función Mass Mailer Atack para llevar a cabo el envío masivo de correos.

6. **Análisis de datos cuantitativos:**
   - Se analizaron los datos cuantitativos recopilados en la encuesta para determinar la frecuencia, los patrones y las características del spam masivo en los clientes de ISPs en el cantón Huaquillas.
   - Se identificaron posibles correlaciones o tendencias entre la recepción de spam masivo y las vulnerabilidades de seguridad identificadas.

7. **Análisis de datos cualitativos:**

- Explorar las experiencias, percepciones y recomendaciones de los clientes de ISPs en relación con la seguridad y el spam masivo.

8. **Interpretación de los resultados:**
   - Interpretar los resultados del análisis estadístico para comprender las vulnerabilidades identificadas y su impacto en los clientes de los ISPs en el cantón Huaquillas.

9. **Conclusiones y recomendaciones:**
   - Resumir las conclusiones basadas en los hallazgos y responder a las preguntas de investigación planteadas.
   - Formular recomendaciones prácticas y acciones concretas para mitigar las vulnerabilidades identificadas, mejorar las medidas de seguridad y proteger a los clientes de ISPs en el cantón Huaquillas.

En el proceso de aplicación de la encuesta, se seleccionó una muestra representativa siguiendo el marco metodológico establecido. La tabla 1 presenta la cantidad de personas encuestadas para cada proveedor de servicios de internet en el cantón Huaquillas:

Resultados

Descripción de la muestra

Tabla 1:
Descripción de la población total

Empresas	Población
Techmesh	35
Netlik	35
Ipnet	25
+FiberHome	69
Alfa & Omega	25
Digitalnet	35
Telsisnet	30
TV Oro	35
Gonet	25
AlphaNet	25
ETR solutions	15
Intersur	15
TOTAL	**369**

Nota. Se tomó en consideración los siguientes ISPs debido a que son los principales y más conocidos en el cantón. Fuente: El autor.

Con el propósito de investigar si la población bajo estudio, estipulada en la Tabla 1, es víctima de algún tipo de ataque, se seleccionó una muestra representativa. Los ataques se llevaron a cabo a través de correos electrónicos siendo éste el medio principal. En cuanto al contenido del mensaje, decía lo siguiente:

Figura 1:
Cuerpo del correo electrónico

Fuente: Fuente propia.

Nota. Correo Electrónico enviado al buzón de entrada de cada correo registrado en las encuestas

Medio de ataque: correo electrónico

Análisis de los Resultados

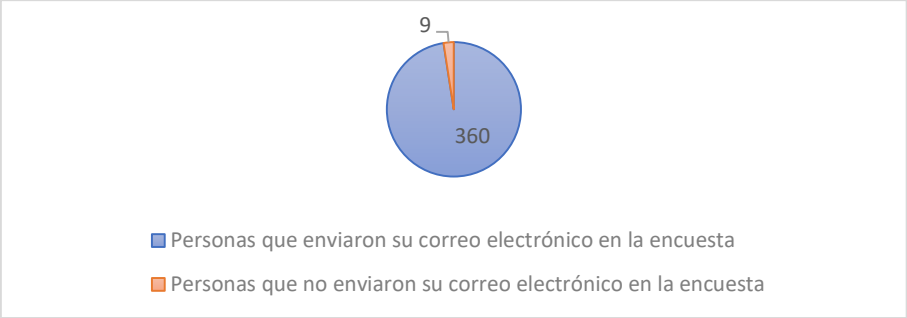
Para el desarrollo del proyecto, se implementó el primer escenario que consistió en una encuesta sobre la calidad del servicio de Internet. Se incluyó un campo opcional para recopilar las direcciones de correo electrónico de los encuestados, lo cual resultó útil para el segundo escenario.

Tabla 2:
Resultados obtenidos de la encuesta

Población	Cantidad
Personas que enviaron su correo electrónico en la encuesta	360
Personas que no enviaron su correo electrónico en la encuesta	9
TOTAL	**369**

Fuente: Fuente propia.

Figura 2:
Personas que enviaron su correo electrónico



Fuente: Fuente propia.

De todas las personas que participaron en la encuesta, un total de 360 individuos proporcionaron su dirección de correo electrónico, mientras que aproximadamente el 2.44% optó por no enviar su dirección de e-mail.

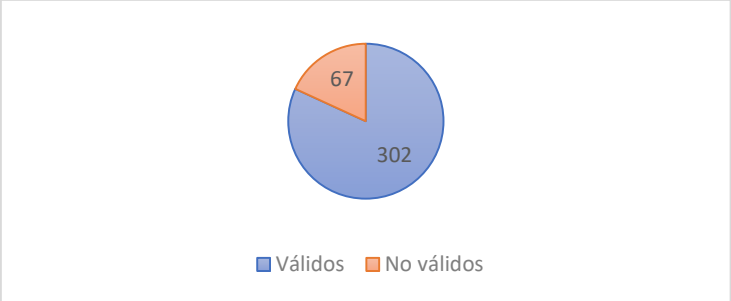
Tabla 3:

Correos electrónicos	Cantidad
Válidos	302
No válidos	67
TOTAL	**369**

Validación de correos electrónicos

Fuente: Fuente propia.

Figura 3:
Correos electrónicos



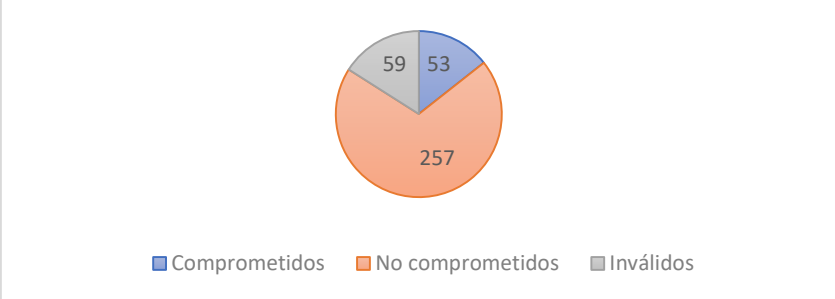
Fuente: Fuente propia.

En función de esta información, se puede inferir que la mayoría de los correos electrónicos ingresados en el estudio son válidos, lo cual es un resultado positivo. Sin embargo, el porcentaje de correos inválidos todavía representa una proporción significativa, lo que sugiere que existe una cantidad considerable de errores o información incorrecta en los datos recopilados.

Correos electrónicos	Cantidad
Comprometidos	53
No comprometidos	257
Inválidos	59
TOTAL	**369**

Tabla 4:
Resumen de correos comprometidos
Fuente: Fuente propia.

Figura 4:
Correos comprometidos



Fuente: Fuente propia.

Basándonos en los resultados de esta tabla, notamos que existe una proporción considerable de correos electrónicos comprometidos debido a ataques de phishing. Esto sugiere la existencia de una posible vulnerabilidad en la seguridad y resalta la necesidad de tomar medidas para proteger la información personal y evitar caer en estafas.

Discusión

El cantón Huaquillas, ubicado en la provincia de El Oro, según INEC (2019) "tiene un total de 48.285 habitantes, 24.165 son mujeres y 24.120 son hombres" (p. 1), este número de población es importante tenerlo en cuenta al analizar las vulnerabilidades a través de spam masivos en los clientes de los proveedores de servicios de Internet (ISPs) en esta región.

Ecuador es un país con 18 millones de habitantes, de los cuales el 77% son usuarios de Internet. Hay 15.91 millones de celulares en el país y 81% de la población es usuaria activa en redes sociales, es decir, hay más perfiles en redes sociales que usuarios conectados diariamente a Internet. El 76% de la población usa internet activamente. Por su parte, el 98% de los usuarios de redes sociales accede a Internet desde sus celulares. El número de usuarios de Internet en Ecuador se incrementó 65% en una década (del 2012 al 2022) pasando de 4.8 a 13.6 millones. (Medina, 2022)

En la era digital en la que vivimos, el phishing se ha convertido en una de las amenazas más comunes y persistentes en línea. Dávalos (2021) menciona que se ha observado una disminución en los ataques de phishing (mensajes fraudulentos), sin embargo, varios países de la región continúan siendo los más afectados a nivel mundial. En términos de la proporción de usuarios que han sufrido ataques durante los primeros ocho meses del año, Brasil ocupa el primer lugar con un 15,3% de personas afectadas. Le siguen Ecuador con un 13,3% de usuarios impactados y Panamá con un 12,6%. Por otro lado, Venezuela (7,19%) y la República Dominicana (5,62%) se encuentran entre los países con menor incidencia de ataques de ingeniería social a nivel global.

Aunque se ha observado una disminución general en los ataques de phishing, varios países de la región siguen siendo los más afectados a nivel mundial, incluyendo a nuestro país, esto indica que aún existe una vulnerabilidad significativa en la conciencia y las prácticas de seguridad en línea de los usuarios.

Los ciberataques están en constante aumento y sus cifras se incrementan día a día, convirtiéndose en una de las amenazas en línea más frecuentes y persistentes. Según Softtek (2018): Los ciberataques a nivel mundial; en primer lugar, se encuentra el correo spam, elevándose el porcentaje a un 83%, le sigue los virus/malware cuya función es inutilizar sistemas y dispositivos (62%) y el popular ramsonware con un porcentaje del 33%, por último, el espionaje industrial, así como los ataques destinados a los sistemas de control y producción representa tan sólo un 1%. Además, de acuerdo con Deloitte, ya que gran parte de los ataques se basan en ingeniería social, la concienciación, formación y el entrenamiento de los empleados es uno de los mayores métodos defensivos frente a los posibles ataques.

En el ámbito nacional, Chang (2020) menciona que:

En junio del año 2017, Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. El 49,05 % de estos fueron ocasionados por ataques de fuerza bruta (denominado Bruteforce Generic RDP) a servidores de RDP. En Ecuador el 43 % de los ciudadanos tiene acceso a internet, sin embargo, la gran mayoría, desconocen medidas de protección y prevención sobre las amenazas y peligros de su uso, debido a que carecen de una educación formal sobre el tema informático, siendo fácilmente víctimas de los ciberataques; por otro lado, las políticas de ciber seguridad en las empresas del Ecuador, tampoco se aplican de manera rigurosa.

Para el desarrollo del proyecto, se implementó el primer escenario que consistió en una encuesta sobre la calidad del servicio de Internet. Se incluyó un campo opcional para recopilar las direcciones de correo electrónico de los encuestados, lo cual resultó útil para el segundo escenario.

Conclusiones

Según los resultados de las encuestas aplicadas en esta investigación, existe una presencia significativa de spam masivo en los clientes de ISPs en el cantón Huaquillas, lo que representa una amenaza para la confidencialidad y la integridad de la información personal y empresarial.

Los cibercriminales continúan desarrollando técnicas sofisticadas de spam y phishing, lo que dificulta su detección y prevención. Esto requiere una constante actualización y mejora de las medidas de seguridad por parte de los ISPs.

La educación y concientización de los usuarios son fundamentales para prevenir caer en trampas de phishing y estafas. La implementación de programas de educación y la divulgación de buenas prácticas de seguridad en línea pueden reducir la exposición de los usuarios a los riesgos del spam masivo.

Es crucial que ISPs y usuarios tomen medidas proactivas contra spam y vulnerabilidades. Esto incluye implementar tecnologías de seguridad, capacitar usuarios y colaborar en seguridad cibernética para lograr un entorno en línea seguro y confiable en Huaquillas.
Setoolkit resultó ser una herramienta altamente poderosa y versátil que ofrece diversas funcionalidades para realizar pruebas de penetración y evaluaciones de seguridad en entornos controlados y con el consentimiento de los propietarios de los sistemas. Sin embargo, es importante tener en cuenta que el uso de Setoolkit y otras herramientas similares debe ser ético y legal.

Referencias bibliográficas

Angulo, S. (12 de diciembre de 2021). Expreso. Obtenido de https://www.expreso.ec/actualidad/economia/ecuador-top-20-paises-llamadas-comerciales-deseadas-118196.html

Astudillo, E. B. (15 de noviembre de 2019). UNEMI. Obtenido de https://www.redalyc.org/journal/5826/582661898003/html/

Chavez, J. J. (3 de marzo de 2023). Delta Protect. Obtenido de https://www.deltaprotect.com/blog/vulnerabilidad-informatica

Cuenca, C. (1 de febrero de 2019). UTPL. Obtenido de https://csirt.utpl.edu.ec/node/275

Dávalos, N. (14 de noviembre de 2021). Primicias. Obtenido de https://www.primicias.ec/noticias/tecnologia/ciberataques-latinoamerica-elevan-pirateria-trabajo-remoto/

Diaz, J. P. (2021). Ingenieria Social, un ejemplo practico. REVISTA UISRAEL, 54.

Granado, H. D. (31 de Agosto de 2021). KASPERSKY. Obtenido de https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

INEC. (16 de mayo de 2019). Obtenido de https://www.ecuadorencifras.gob.ec/censo-de-poblacion-y-vivienda/

International IT. (11 de enero de 2022). Obtenido de https://www.internationalit.com/post/los-ciberataques-aumentaron-un-50-en-2021?lang=es

ISO Tools. (11 de marzo de 2021). Obtenido de https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Medina, R. (6 de septiembre de 2022). Branch. Obtenido de https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-en-ecuador-2021-2022/#:~:text=Ecuador%20es%20un%20pa%C3%ADs%20con,usuarios%20conectados%20diariamente%20a%20Internet.

Quezada Lucio, N. (2019). Metodología de la investigación (Primera ed.). Lima: Macro E.I.R.L.

Softtek. (21 de mayo de 2018). Obtenido de https://blog.softtek.com/es/el-desconocimiento-es-la-mayor-amenaza-a-la-ciberseguridad

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.