Conocimiento de la percepción de la ciberseguridad en los estudiantes de la escuela de Economía de la Universidad de Costa Rica en su vida cotidiana, con enfoque a redes sociales

Knowledge of the perception of cybersecurity in the students of the school of economics of the University of Costa Rica in their daily lives with a focus on social network

María Paz Castro-López[1]

Castro-López, M.P. Conocimiento de la percepción de la ciberseguridad en los estudiantes de la escuela de economía de la Universidad de Costa Rica en su vida cotidiana, con enfoque a redes sociales. *Tecnología en Marcha*. Vol. 37, número especial. Julio, 2024. XI Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software, Salud Electrónica y Móvil (AmITIC). Pág. 5-11.

https://doi.org/10.18845/tm.v37i6.7261

1 Estudiante. Universidad de Costa Rica. Costa Rica.
mariapaz.castro@ucr.ac.cr
https://orcid.org/0009-0005-2527-5945

Palabras claves

Ciberseguridad; redes sociales; *Phishing*; suplantación de identidad; accesos seguros.

Resumen

La presente investigación tiene como objetivo realizar un análisis exploratorio con relación al conocimiento que poseen los estudiantes del curso de Economía de la Universidad de Costa Rica con respecto a su uso de la Ciberseguridad en redes sociales en sus cuentas personales y cómo se accede a ellas de forma adecuada. Luego se plantea una guía rápida que contiene una serie de pasos que se recomiendan para incrementar el conocimiento del tema y lograr establecer mejoras sobre el uso de las redes sociales, accesos seguros y técnicas de Suplantación de identidad que se pueden dar en esas redes.

Keywords

Cybersecurity; social networks; Phishing; identity theft; secure access.

Abstract

The objective of this research is to carry out an exploratory analysis in relation to the knowledge that students of the UCR Economics course have regarding their use of Cybersecurity in social networks in their personal accounts and how to access them properly. Then a quick guide is proposed that contains a series of steps that are recommended to increase knowledge of the subject and achieve improvements in the use of social networks, secure access and impersonation techniques that can occur in these networks.

Introducción

La aplicación de la ciberseguridad se ha convertido en una necesidad para la protección de la información de todos los usuarios que posean algún tipo de aplicación electrónica o móvil, precisamente porque se desea detectar vulnerabilidades en dichos programas o plataformas que se podrían llegar a utilizar en contra del usuario, como los es el robo de datos. Si bien en el campo de las redes sociales el robo de datos varía en comparación a otras aplicaciones, ya que es el usuario el que expone sus datos al público ya sea por medio de comentarios, publicaciones o historias. Sin embargo, esto no le quita importancia de que se debe tener conocimiento de todas aquellas maneras seguras navegar en estos programas, incluso profundizar cómo estas podrían variar según la plataforma utilizada.

Una de las poblaciones que hace un mayor uso de las aplicaciones sociales es la estudiantil. Ya que en su día a día buscan poder estar conectados unos con otros, así como con el mundo externo. En el presente las redes sociales son nuestro mundo actual en el que realizamos una variedad de actividades como es darnos a conocer, mejorar nuestra imagen para todos aquellos usuarios que nos siguen así como para fortalecer relaciones entre usuarios. Esto ha sido de gran impacto para el desarrollo social alrededor del mundo ya que como nos visualizan como persona se basa en cómo nos presentamos en las redes.

Estos medios de los cuales somos muy partícipes requieren seguridad ya que al no ser aplicada de forma correcta puede tener repercusiones a largo plazo. Robo de identidad, cyberbullying, robo de contraseñas son algunas de las incidencias que pueden ser generadas por la falta de

conocimiento de la seguridad que se debe tomar en cuenta en estas plataformas. Es por esto que informarse de ciberseguridad. y aplicar lo aprendido va a ser un gran beneficio para toda persona que utilice las redes sociales. [4]

Materiales y métodos

El enfoque del tipo de investigación de este artículo es cualitativo ya que, el propósito es examinar la forma en que ciertos individuos perciben y experimentan fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados [1]. Acerca de la caracterización del estudio se establece que sea de tipo exploratorio, el cual se basa en conocer una problemática de la cual no se evidencia amplio estudio previo, así como definir conceptos y priorizar los puntos de vista de las personas que participan en el proceso. Este estudio permitirá obtener información para una investigación posterior más completa de la cual se desea implementar el plan de acción a la población estudiada. Con respecto a los materiales se aplicó una encuesta a todos los compañeros de la clase 20 aproximadamente, este documento tenía 10 preguntas las cuales iban a evaluar el conocimiento de la población en relación a diferentes tópicos de ciberseguridad. Luego de las respuestas obtenidas se tabulan los datos y se muestran los gráficos más representativos. Entre ellos están los siguientes:

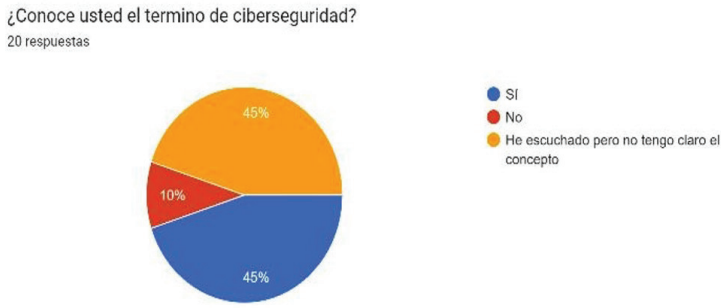

Figura 1. Conocimiento del término ciberseguridad.

En la figura 1 se muestra que el 10% indica que no conoce el tema, y el 45% indica que ha escuchado, pero no tiene claro el concepto y un 10% que no tiene conocimiento alguno del término.

Figura 2. El uso de la red socal que más frecuentan.

Con respecto a la figura 2 se muestra cuáles son las redes más usadas, donde el 55% de la población indica que Instagram.

Figura 3. Conocimiento de lo que es una contraseña segura.

En la figura 3 se muestra que 30% de la población indica que no sabe que es una contraseña segura.

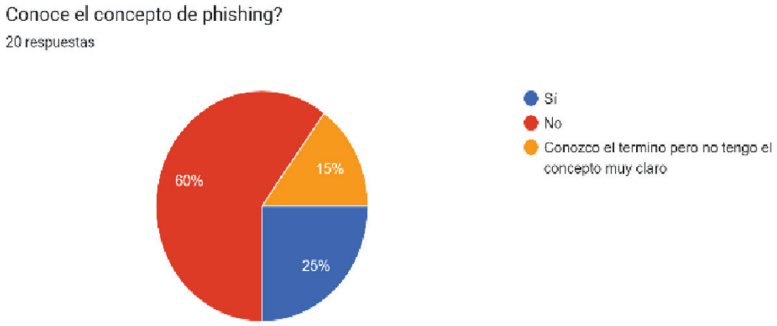

Figura 4. Conocimiento del término *Phishing*

Como se muestra en la figura 4 el 60% indica que no conoce el concepto de Phishing y el 15% indica conocer el termino, pero no tiene el concepto claro. Y solo el 25% posee conocimiento del termino.

Propuesta

Luego de ver los resultados más representativos se plantea una guía que muestra el detalle de algunos conceptos importantes y de acciones puntuales que se deben realizar con respecto a la seguridad en las redes sociales así como los son las contraseñas seguras, técnicas de suplantación y cómo realizar una autenticación segura, así como lo que es el concepto de ciberseguridad , phishing y cómo estos se ven reflejados en las redes sociales. Y finalmente el uso de los correos electrónicos y la forma de verificar su autenticidad.

Cuadro 1. Guía rápida para el uso en redes sociales

Criterio	Concepto y Acciones
Ciberseguridad	La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o interrumpir la continuidad del negocio. Según [2]. Sus principales campos para actuar son la seguridad de red, seguridad de la nube y la seguridad física. En redes sociales es esencial ya que la cantidad de información que se expone en ellas podría utilizarse de manera maliciosa, especialmente si se llegara a concretar algún ataque. La vinculación de estos datos personales con otras plataformas de servicios puede ocasionar daños indirectos con los mismos si se logra un ataque exitoso, he de aquí su importancia. [7]
Contraseñas seguras	El objetivo de una contraseña segura para evitar que otra persona acceda a su cuenta y proteger los datos personale**s** [8]**, es** por eso que se recomienda**:** No utilizar contraseñas cortas, no nombres personales, de mascotas, de uso común o contraseñas ya antes utilizadas en otras aplicaciones.. No usar patrones tan simples como “123456” o “Qwrty” que están en el teclado. Utilizar combinaciones de varias palabras, que, aunque aparentemente no tengan relación lógica entre ellas se puedan recordar como “Perro azul 3000”. Combinar mayúsculas, minúsculas, números y caracteres especiales, así como “Felicidad 2023$”. Por último utilizar un medidor de fortaleza de contraseñas: https://lowe.github.io/tryzxcvbn/ para confirmar si la contraseña es lo suficientemente segura o se podría mejorar aún más. Así como también el uso de generadores de contraseñas como lo es https://www.dashlane.com/es/features/password-generator es de gran ayuda en el caso de que crear una contraseña propia no se pueda lograr con sus propios medios.
Phishing	Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o archivo que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo. Sinónimo: Vishing, Smishing. Según [3] **No utilizar correo** de procedencia extraña con un link. Verificar el encabezado y la firma que pertenece a una organización. No atender correos con solicitudes de ayuda, cambio de credenciales, cambio de configuraciones o solicitudes específicas.[5] a menos de que el usuario lo necesite de lo contrario la mayoría de plataformas sociales o que brindan servicios no solicitan este tipo de datos, es por esto que si se recibe un correo solicitando ese tipo de información se debe tratar de forma cuidadosa. Además, el phishing se ve reflejado de diferentes formas dependiendo de la plataforma en la que se esté aplicando como lo es en el caso de Instagram. Según [9]. En esta aplicación un ataque de phishing inicia cuando un ataque genera una página falsa de inicio de sesión en Instagram. Su objetivo es parecerse lo más posible a la página original, así que cuando el cliente ingresa su usuario de Instagram junto con su contraseña el atacante obtendrá sus datos los cuales los puede utilizar para hacerse pasar por su persona en las redes o robar información facilitada en las mismas. Es por eso que se debe confirmar si las páginas de inicio de sesión son las verdaderas, verificando su link de procedencia que no posea nada fuera de lo común e incluso comprarlo con el original para asegurarse de que sea el indicado. En el caso de Facebook un ataque de phishing se ve reflejado por medio de un mensaje o link el cual le solicita que le de confirmación a su información personal. Estos mensajes son entregados a través de la misma plataforma o facebook messenger [9]. Esto es un caso más difícil de diferenciar, sin embargo, en el caso de mensajes es bueno confirmar si realmente es un amigo de la plataforma consultándole, pero lo más importante es evitar a toda costa ingresar directamente al link de procedencia sin haber confirmado que es legítimo.
Autenticación	Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico etc. Autentificación o autenticación básica: Definición Esquema de autenticación basado en la web más simple que funciona

Criterio	Concepto y Acciones
	Mediante el envío del nombre de usuario y contraseña con cada solicitud o con un código de letras o números. Utilizar factor de doble autenticación con Google u otra cuenta de correo que se utilice. En los accesos a cuentas de banco utilizar un token u otra combinación de códigos que garantice que solo la persona conoce cómo ingresar y tiene las credenciales necesarias. En el caso de algunas plataformas sociales se recomienda utilizar también algún número telefónico de confianza del cual se pueda verificar la identidad del usuario.
Seguridad redes sociales	¿Cómo configurar los ajustes de privacidad y seguridad en Instagram? Activar la autenticación en dos pasos para mejorar la seguridad de la cuenta [10] [11]. Nunca dar la contraseña a alguien que no conoces o en quien no confías. Piensa antes de autorizar a una app de terceros. Elige una contraseña segura y única que no uses para otras cuentas. Usa una combinación de al menos seis números, letras y caracteres especiales (como !$@%), e intenta evitar repeticiones. Cambiar la contraseña periódicamente, en especial si hay un mensaje de Instagram donde se pide que lo hagas. Cambiar las contraseñas de todas las cuentas de correo y no usar la misma contraseña en más de una cuenta. Descarga tus datos. Cierra sesión en Instagram cuando uses una computadora o un teléfono que compartes con otras personas. Si inicias sesión desde una computadora pública, no marques la casilla “Recordarme”, ya que, al hacerlo, permaneces conectado incluso después de cerrar la ventana del navegador.
Suplantación de identidad	Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Según [3] Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella. Revisar los perfiles de solicitud, buscar información, fotos que aseguren que esa persona es quien dice ser. Buscar otros medios para verificar la autenticidad de los datos, información cruzada de otro perfil u otro sistema.

Conclusiones

Antes los resultados encontrados se propone una guía de uso para la vida cotidiana con enfoque a la ciberseguridad en las redes sociales, dicha guía incluye lo que es una contraseña segura sea una contraseña diferente con respecto a sus otras redes sociales, que tengan una combinación entre números, letras, mayúsculas y caracteres. Además, su mayor objetivo es proteger la información del usuario; con esto se incluye correos electrónicos, archivos y demás contenido. Así como puede identificar por cuenta propia su red social de mayor uso con el objetivo de leer los acuerdos de privacidad y la información, y como estas normativas cumplen su función en relación con el uso. Por último, recalcar las diferentes importancias del uso de las contraseñas seguras y cómo estás mejoran nuestra interacción con las redes y sus elementos que la componen.

Referencias

[1] Hernández-Sampieri, R., & Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Mcgraw-hill.

[2] https://www.cisco.com/c/es_mx/products/security/what-iscybersecurity.html. Recuperado el 09 de julio 2023.

[3] www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ ciberseguridad_2021.pdf. Recuperado el 05 de Julio 2023.

[4] López Mendoza, A., Roque Hernández, R. V., Prieto Quezada, M. T., & Salazar Hernández, R. (2022). Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y, Z: Un estudio comparativo de dos universidades públicas en México. Dilemas Contemporáneos: Educación, Política y p. 301, 1982].

[5] Muñoz Andrade, A. N., Morales Carvajal, A. J., Parra Cantor, L. R., & Pino Mahecha, S. C. (2022). El phishing un adversario silencioso en la comunidad universitaria Ean.

[6] Del Estado De Hidalgo, U. A. (s. f.). *La investigación cualitativa*. https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n3/e2.html Recuperado el 30 de noviembre 2023.

[7] Seguridad, R. R. (2023, 14 noviembre). La ciberseguridad en redes sociales: los riesgos y cómo mantenerse a salvo - Revista Seguridad 360. *Revista Seguridad 360*. https://revistaseguridad360.com/noticias/ciberseguridad-en-redes-sociales/

[8] *Cómo crear una contraseña segura y tener una cuenta más protegida - ayuda de cuenta de Google*. (s. f.). https://support.google.com/accounts/answer/32040?hl=es-41 Recuperado el 30 de noviembre de 2023.

[9] ¿Qué es el phishing en redes sociales? (s. f.). Trend Micro. https://www.trendmicro.com/es_mx/what-is/phishing/social-media-phishing.html Recuperado el 30 de noviembre de 2023

[10] *Facebook*. (s. f.). https://es-la.facebook.com/help/148233965247823 Recurado el 30 noviembre de 2023

[11] Instagram - autenticación en dos pasos (2FA). (s. f.). Privacy International. https://privacyinternational.org/es/guide-step/3867/instagram-two-factor-authentication Recuperado el 30 noviembre del 2023