

## **El phishing un adversario silencioso en la comunidad universitaria Ean**

**Morales, A; Muñoz, A; Parra, L; Pino, S**

amorale29586@universidadean.edu.co; amunoza72114@universidadean.edu.co;

lparraca7338@universidadean.edu.co; spinoma62529@universidadean.edu.co

### Resumen

En la actualidad es cada vez más fácil el acceso de las personas al internet, con el aumento de los usuarios en la internet también se han incrementado los ciberataques de los que pueden ser víctimas los usuarios, estos pueden darse debido a descuidos o vulnerabilidades que no todas las personas son capaces de detectar a tiempo. Los jóvenes son quienes tienen mayor vulnerabilidad, pues son quienes pasan mayor parte del tiempo frente a las pantallas, ya sea por motivos de ocio o de estudio. La comunidad Ean no está exenta de los ataques de los ciberdelincuentes, los estudiantes son los más vulnerables, el ciberataque del que pueden ser víctimas principalmente es el phishing.

Palabras claves: Phishing, Seguridad informática, ciberdelincuencia.

### **ABSTRACT**

Nowadays, it is becoming easier for people to access the internet, with the increase in users on the internet, cyberattacks of which users can be victims have also increased, these can occur due to carelessness or vulnerabilities that do not all people are able to detect in time. Young people are the most vulnerable, since they are the ones who spend most of their time in front of screens, either for leisure or study. The Ean community is not exempt from attacks by cybercriminals, students are the most vulnerable, the cyberattack they can be victims of is mainly phishing.

Keywords: Phishing, Informatic security, cybercrime.

## **Introducción**

Hoy en día las computadoras, como el teléfono móvil son parte indispensable del día a día, y es difícil imaginar la vida sin ellos, pero para llegar a tener los servicios que nos ofrecen las computadoras y el internet en la actualidad se debió pasar por años de desarrollo, y así como se mejoró el acceso al internet también surgieron quienes quieren obtener un provecho del mismo.

Hernández, L. da a conocer que, durante la década de los setenta, la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia económica, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc. Hasta el punto que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos, éstas eran las principales manifestaciones del mismo.

Actualmente las TIC's han llegado a la mayor parte de la sociedad, y la actual pandemia ha extendido su uso, por lo tanto, la educación se está transformando constantemente para lograr estar a la vanguardia. En concordancia con Flores. M, las nuevas generaciones necesitan del uso de la tecnología y se les debe dirigir creando un proceso integral de enseñanza y aprendizaje. Por lo que, también se les debe instruir para evitar que caigan en manos de los ciberdelincuentes.

El ambiente educativo no es ajeno a este tema, este también ha cambiado a medida que se han adoptan nuevas tecnologías, este proceso genera oportunidades de mejora que las organizaciones adoptan con el fin de potencializar su gestión, según ESET (2014). Se esperaba que para el año 2016, un 36% de la información de los usuarios estuviese almacenada en la nube, cifras que a la actualidad han seguido en aumento. Debido a la gran cantidad de datos que debe almacenar la nube ha surgido la necesidad de implementar controles y procedimientos a través de normas y marcos de trabajo, esto con el fin de minimizar los riesgos y pérdidas de información.

El contexto en el que se desarrolló el presente documento fue el educativo, la finalidad es determinar como el phishing afecta a la comunidad Eanista, especialmente a los jóvenes quienes son los más vulnerables y algunos desconocen esta metodología de fraude.

### **Marco de referencia**

La importancia que representa el internet en la vida cotidiana es indiscutible, para acceder a él solo basta sacar el móvil del bolsillo y conectarse. Sin embargo, en sus inicios el internet no era fácilmente accesible, se requería de equipos voluminosos y especializados, además de complejos comandos para interactuar con él. El advenimiento de la computadora personal fue el desencadenante de la masificación del internet, no obstante, para que las computadoras llegaran a ser lo que son hoy en día pasaron por diferentes etapas de desarrollo, en el principio era tecnología usada por la inteligencia militar, más adelante por las grandes empresas, entre las décadas de 1950 a 1990 se dieron grandes pasos, así mismo surgieron nuevas empresas fabricantes tanto de computadoras, como de componentes, algunas de ellas se mantienen hoy en día, como ejemplo, tenemos a las grandes conocidas como lo son Apple, Microsoft e Intel. Hoy en día las personas del común pueden tener un fácil acceso a la compra de microcomputadoras, computadoras de escritorio, computadoras portables, no obstante, todavía hay tecnología que pertenece a las grandes empresas como por ejemplo las supercomputadoras.

Las computadoras e internet se han ido desarrollando de manera exponencial, así mismo también se amplió la capacidad de almacenamiento de la información, y la capacidad de transportarla. La mayor parte de los usuarios hoy en día son capaces de manejar un artefacto de manera simple, los usuarios pueden acceder fácilmente a la red teniendo un dispositivo con conexión, no obstante, existe partes programables de las cuales solo una pequeña porción de la población mundial es capaz de dominar y es debido a ello que los criminales aprovechan para atacar por medio de la red a personas o instituciones.

Hernández (2009) nos da a conocer que, durante la década de los setenta, la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia

económica, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc. Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos, éstas eran las principales manifestaciones del mismo.

Actualmente las TIC's han llegado a la mayor parte de la sociedad, y la actual pandemia ha extendido su uso, por lo tanto, la educación se está transformando constantemente para lograr estar a la vanguardia, en concordancia con Flores. M, las nuevas generaciones necesitan del uso de la tecnología y se les debe dirigir creando un proceso integral de enseñanza y aprendizaje. Por lo tanto, también se les debe instruir para evitar que caigan en manos de los ciberdelincuentes.

## **Metodología**

### **Tipo de investigación**

De acuerdo con las rutas de investigación expuestas por Hernández, R. y Mendoza, C. P., para este proyecto se decide seguir la ruta de tipo cualitativo – descriptivo, pues con el desarrollo del mismo lo que se pretende es examinar el comportamiento de la población estudiantil de la Universidad Ean acerca del phishing a partir de preguntas orientadoras que generen información relevante que posteriormente será analizada con el propósito de elaborar un informe de resultados que permita evaluar el nivel de conocimiento de los estudiantes sobre esta modalidad de ciberdelincuencia

### **Población y muestra**

Debido a que este proyecto se enmarca dentro de la comunidad académica los participantes del presente proyecto de investigación tienen como principales características de inclusión ser estudiantes de la universidad Ean de pregrado de la modalidad virtual, el muestreo fue de tipo probabilístico por conveniencia. El tamaño de la muestra fue de 34 participantes teniendo en cuenta que la población fue de 1370 que cumplieran con la característica de inclusión ya descrita anteriormente, esta muestra tiene una confianza del 90 % y un margen de error del 14 %.

## **Procedimientos**

El presente proyecto de investigación se desarrolló siguiendo los procedimientos descritos a continuación:

**Fase 1. Planteamiento del problema.** En la presente fase se identificó un problema que entorno a un grupo de participante y un contexto específico.

**Fase 2. Marco de referencia.** Se construyó el marco teórico teniendo en cuenta diferentes fuentes bibliográficas y el estado del arte del tema tratado.

**Fase 3. Construcción del instrumento.** Se selecciono la herramienta e instrumento a desarrollar se creó un formulario de Google para la construcción del instrumento, teniendo en cuenta que esta herramienta permitía la fácil divulgación del instrumento.

**Fase 4. Aplicación del instrumento.** Por medio de redes de comunicación como correo institucional y WhatsApp se compartió el instrumento a los estudiantes de pregrado virtual de la universidad Ean con el fin de obtener una muestra que permitiera validar los objetivos de la investigación.

**Fase 5. Análisis de Datos.** Después de obtener la muestra que nos diera un nivel de confiabilidad del 90%, se procedió al análisis de los datos tanto socio demográficos como los de percepción sobre el phishing.

## **Instrumento**

El instrumento que se utilizó para la recolección de datos fue por medio de encuestas, las cuales incluía una por un lado preguntas sociodemográficas y preguntas sobre la percepción del phishing y por otro lado se replicó una encuesta realizada por Google en la cual se exponen a los participantes una serie de correos que permiten su exploración con el fin de identificar si se trata de un intento de phishing o si es un correo real.

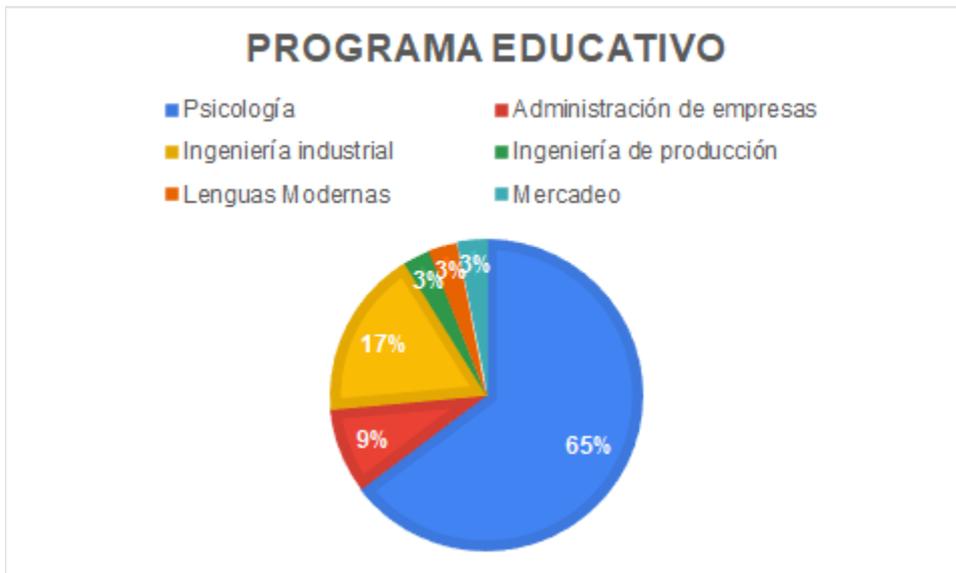
Encuesta: <https://forms.gle/5NaYsdugh6nyaNGn8>

## Resultados de la investigación

A continuación, se realiza el procesamiento y análisis de datos de acuerdo a los resultados obtenidos en la encuesta realizada a los estudiantes.

Después de la recolección de datos se obtuvo una participación del 65% de estudiantes de psicología, 17% de Ingeniería industrial, 9% de administración de empresas, y 3% de Ingeniería de producción, Lenguas modernas y mercadeo respectivamente, para un total del 100%.

Grafico. Programa educativo.



Fuente: Elaboración propia.

Se les enseñó a los participantes del estudio un video, en el cual se les daba a conocer el termino phishing, con la finalidad de que se familiarizarán con el término y pudieran seguir con la encuesta.

Se indagó dentro de los participantes si habían sido alguna vez víctimas del phishing y se obtuvo como resultado que un 18% lo habían sido, mientras que un 82% aseguró no haberlo sido.

Grafico. Víctima del phishing.



Fuente: Elaboración propia.

Se indagó dentro de los participantes si conocían previamente sobre el phishing o tenían alguna idea de lo que significaba caer en este tipo de estafa, 18% no lo conocía, mientras un 82% si lo conocía.

Grafico. Conocimiento sobre el phishing.

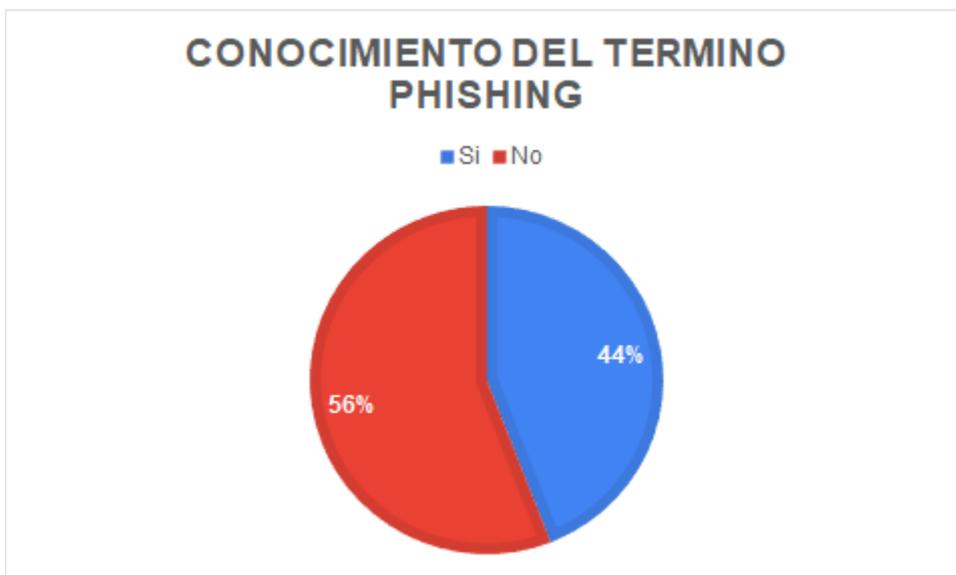


Fuente: Elaboración propia.

De acuerdo a los dos gráficos anteriores, se podría concluir que la mayoría de las personas de la comunidad educativa Ean, tiene conocimiento sobre el término del phishing y cómo esta modalidad les afecta, también se podría decir que su conocimiento se debe a que son personas jóvenes, que han crecido con acceso a internet, y esto ha permitido que desarrollen mayor discernimiento sobre como tener seguridad dentro de la web. También se puede concluir que si las personas conocen sobre el termino y sobre ciberseguridad son menos propensas a ser víctimas del cibercrimen.

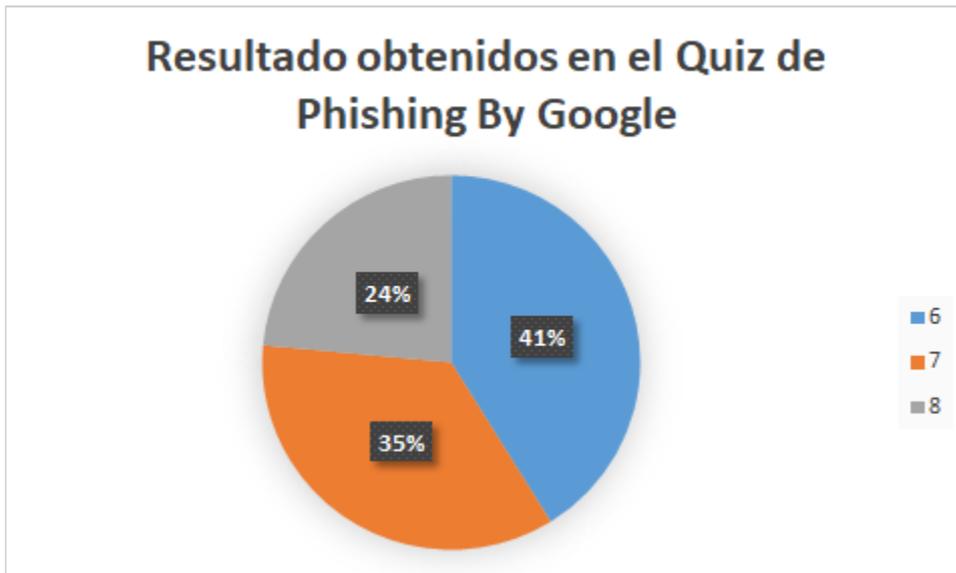
Se indagó dentro de los participantes si conocían previamente el termino de phishing, 44% aseguro conocerlo, mientras un 56% no.

Gráfico. Conocimiento del término phishing.



Fuente: Elaboración propia.

Gráfico. Resultados obtenidos en el Quiz de phishing By Google



Fuente: Elaboración propia.

El Gráfico anterior nos permite evidenciar que aun cuando el 100% de los participantes es obtuvo un puntaje igual y superior a 6 en una escala de 0 a 8, distribuidos de la siguiente manera: el 41% que corresponde a 14 participantes obtuvieron una puntuación de 6, el 35% es decir 12 participantes obtuvieron 7 respuestas correctas y el 24% que corresponde a 8 participantes obtuvieron las 8 respuestas correctas, esto nos permite concluir que la probabilidad que estudiantes de la universidad Ean sean víctimas de phishing.

## Conclusiones

Los jóvenes al ser quienes pasan mayor tiempo delante de las pantallas son quienes tienen mayor vulnerabilidad ante los ciberdelincuentes, dentro de este público es en su mayoría desconocido el phishing, no obstante, a medida que la persona va conociendo más sobre el internet es más consciente de las posibilidades de caer en este ciberdelito. Sin embargo, aún es difícil para todos identificar si se trata de un ataque o es algo real, esto debido a la falta de conocimiento y difusión de estos tipos de ataques, por ese motivo es importante enseñar a los jóvenes sobre ciberseguridad, pues al ser ellos quienes son más susceptibles de este tipo de engaños, necesita una educación en el uso apropiado de las TIC's.

Mediante el presente estudio se pudo determinar que, si bien la comunidad estudiantil eanista demuestra un conocimiento general acerca de las modalidades de ciberdelincuencia, al momento de enfrentarse a ellas en un ambiente simulado existen ciertas dificultades para sortearlas. Dichas dificultades pueden ser superadas mediante campañas de divulgación de los riesgos asociados a la ciberdelincuencia y concientización sobre cómo minimizar la posibilidad de ser víctima de ellos.

## Referencias

López, A., García A., Rivera, J., Díaz C. (2018). Jóvenes en la encrucijada digital. Itinerarios de socialización y desigualdad en los entornos digitales. Ediciones Morata. Madrid. España.

Díaz Mohedo, M<sup>a</sup> Teresa & Vicente Bújez, Alejandro (2011). Los jóvenes como consumidores en la era digital.

DDOS. Mapa de ataque digital. (2021). Recuperado de:

<https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18683&view=map>

Penco, A., Platero, A. (2016). La privacidad de los niños y adolescentes en las redes sociales:

Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno. Revista chilena de derecho y tecnología. Disponible en [https://scielo.conicyt.cl/scielo.php?script=sci\\_arttext&pid=S0719-25842016000200063](https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842016000200063)

El diccionario de Ciberriesgo, de la A a la Z. (2021). Willis Towers Watsonupdate. Recuperado de: <https://willistowerswatsonupdate.es/ciberseguridad/diccionario-delciber-riesgo-de-la-a-a-la-z/>

Argüelles, D. (2013). Guía para la presentación de trabajos científicos bajo estándar APA en la Universidad EAN. Bogotá. Publicaciones EAN. Disponible en <https://repository.ean.edu.co/handle/10882/9035>

Hernández, R. y Mendoza, C. P. (2018). Metodología de la investigación. Las rutas cuantitativas, cualitativas y mixtas. México: McGraw-Hill, primera edición. Disponible en <http://repositorio.uasb.edu.bo:8080/bitstream/54000/1292/1/Hern%C3%A1ndez-%20Metodolog%C3%ADa%20de%20la%20investigaci%C3%B3n.pdf>

Redacción EL TIEMPO (2016). La historia detrás de cinco 'hackers' colombianos y sus delitos. El tiempo. Recuperado de: <https://www.eltiempo.com/justicia/cortes/delitosde-hackers-en-colombia-52232>

Consejo superior de la Universidad EAN. Acuerdo 007 del 28 de febrero de 2019. Universidad EAN. Recuperado de: [https://universidadean.edu.co/sites/default/files/institucion/acuerdos/estructura\\_organica](https://universidadean.edu.co/sites/default/files/institucion/acuerdos/estructura_organica)

Lopategui, E. Informática. Historia de las computadoras. Universidad Rafael Landívar. Guatemala. Recuperado de: <http://biblio3.url.edu.gt/Libros/provinciales/computadoras.pdf>

Nebreda, I. (2013) El origen de internet. Universidad Politécnica de Madrid. Escuela de ingeniería y arquitecturas telemáticas. Recuperado de: [http://oa.upm.es/22577/1/PFC\\_IVAN\\_NEBREDA\\_RODRIGO.pdf](http://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pdf)

Simon Film. (2011). Historia de internet. Arpanet. Recurso en video. Recuperado de: [https://www.youtube.com/watch?v=i4RE6dBAjH4&ab\\_channel=simonfilm](https://www.youtube.com/watch?v=i4RE6dBAjH4&ab_channel=simonfilm)

Veá Baró, A. (2002). La historia oculta de internet a través de sus personajes. Universidad Ramon Llull. EALS - Empresa y Tecnología. Recuperado de: <https://www.tesisenred.net/handle/10803/9156#page=1>

López, G. (2002). Tecnologías de internet (De Arpanet a la 3G). Revista Castellano-Manchega de Ciencias Sociales. Recuperado de: <https://dialnet.unirioja.es/descarga/articulo/637885.pdf>

Hernández, L. (2009). El delito informático. Revista Eguzkilore Número 23. Universidad de país Vasco. Recuperado de: <https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf>

Montano, J. (2020). Historia de las TICs: desde su Origen Hasta la Actualidad. Revista digital Lifeder. Recuperado de: <https://www.lifeder.com/historiatics/#:~:text=La%20historia%20de%20las%20TICs,al%20estallar%20la%20revoluci%C3%B3n%20digital.&text=TIC%20son%20las%20siglas%20de,informaci%C3%B3n%20entre%20los%20seres%20humanos.>

Castro, M. Figueroa, G. Vera, D. Álava, J. Parrales, G. Álava, C. Murillo, A. Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Área de innovación y desarrollo, S.L. Recuperado de: DOI: <http://dx.doi.org/10.17993/IngyTec.2018.46>

Flores, M. Ortega, M. (2018). El uso de las nuevas tecnologías: Una estrategia didáctica en los procesos de enseñanza - aprendizaje. Universidad Nacional de Educación a Distancia. Recuperado de: [https://www.researchgate.net/publication/336020345\\_El\\_uso\\_de\\_las\\_nuevas\\_tecnologias\\_una\\_estrategia\\_didactica\\_en\\_los\\_procesos\\_de\\_ensenanza-aprendizaje](https://www.researchgate.net/publication/336020345_El_uso_de_las_nuevas_tecnologias_una_estrategia_didactica_en_los_procesos_de_ensenanza-aprendizaje)

Verdúm, J. C., Jaramillo, D., Cabrera, A., Abad, M., & Torres, A. Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF Definition of Cybersecurity Business Framework based on ADM-TOGAF.