Phishing

Grupo 14

Profesión y Sociedad

Resumen - El importante crecimiento del uso de Internet, además de ayudarnos en nuestro día a día, ha traído consigo que la gente comparta cada vez más su información personal y sus datos. El resultado es que toda esa información personal se vuelve vulnerable a los ciberdelincuentes. El phishing, por tanto, es un ejemplo de ciberdelincuencia que permite engañar a los usuarios, utilizando ilegalmente una organización pública o de confianza en un patrón automatizado para que el internauta confíe en el mensaje, y robar datos relevantes. Los ataques de phishing pueden provocar graves pérdidas a sus víctimas, incluyendo información sensible, robo de identidad, ataques a empresas y secretos gubernamentales.

En este trabajo ahondaremos en las fases y tipos de ataques, vulnerabilidades, amenazas, a su vez que sus objetivos, medios de ataques e investigación de medidas preventivas; haciendo especial énfasis en las organizaciones empresariales.

1. Riesgos detectados y/o su impacto negativo en la sociedad

El phishing es un tipo de delito cibernético en el que el atacante se hace pasar por una fuente confiable para conseguir así que las víctimas les den información personal sensible como nombres de usuario, contraseñas, números de cuentas bancarias, etc. Sin embargo, aunque el phishing más común sea utilizando el correo electrónico, este tipo de ataque puede tomar formas muy diversas y emplear diferentes métodos, pero siempre con el mismo objetivo [1]. A continuación mencionaremos algunos de los tipos de phishing más relevantes:

- El email phishing, como ya hemos mencionado anteriormente, es la manera más común de engañar que utilizan los atacantes. En este tipo de phishing, los hackers se hacen pasar por una identidad u organización legítima para ganarse la confianza de la víctima, y envían correos electrónicos masivos a tantas direcciones como puedan obtener. Normalmente, estos correos se escriben con un sentido de urgencia para así atraer a la víctima a realizar la acción que el atacante desea y obtener su información.[2]

  Un ejemplo de este tipo de phishing sucedió en Sony. Los atacantes obtuvieron información de contacto de empleados de esta compañía a través de Linkedin y realizaron una campaña de phishing por correo electrónico con la que consiguieron más de 100 TB de datos.[3]

- El smishing es un tipo de phishing igual que el email phishing pero que utiliza como medio de difusión los SMS en vez de los correos electrónicos. El resto del funcionamiento del ataque es muy similar al ataque por correo.

  En septiembre de 2020, Tripwire informó sobre una campaña de smishing que se hizo pasar por la Oficina de Correos de los Estados Unidos (USPS). Los atacantes enviaron SMS informando a las víctimas de la necesidad de hacer clic en un enlace para ver información importante sobre una próxima entrega de USPS. El enlace malicioso llevó a las víctimas a varias páginas web diseñadas para robar las credenciales de la cuenta de Google de los visitantes.[2]

- En el spear phishing, al contrario que en el email phishing, el atacante elige las personas a las que ataca. El email o el tipo de ataque que se utilice es personalizado utilizando la información pública que el atacante encuentre sobre las víctimas para así hacer parecer más legítimo el mensaje y que aumente la probabilidad de éxito.[2]

  William Mendez, director general de operaciones de la consultora CyZen, fue objetivo de un ataque de spear phishing. Recibió un email que hacía referencia a una tecnología, CHH, comúnmente empleada por empresas de contabilidad. El correo fue enviado en temporada de impuestos, la época del año en la que este tipo de empresas están más ocupadas normalmente, lo que implica que los usuarios estén ocupados y no presten atención a los correos electrónicos.[4]

- El whaling es un tipo de spear phishing en el que el objetivo es un alto cargo de una compañía, ya que estos pueden acceder a información y recursos que no están al alcance del resto de empleados, por lo que un ataque exitoso de este tipo puede resultar en grandes ganancias para el atacante.[3]

  En 2020, Tessian informó sobre un ataque de whaling cuyo objetivo fue el cofundador del fondo de cobertura australiano Levitas Capital. Recibió un correo que contenía un enlace a Zoom falso, que instaló malware en la red corporativa del fondo y casi provoca una pérdida de 8,7 millones de dólares en facturas fraudulentas. Finalmente, el atacante obtuvo solo 800.000 dólares, pero el daño a la reputación de la empresa hizo que tuviera que cerrar.[2]

- El Business Email Compromise (BEC) es un tipo de estafa dirigida a empresas que realizan transferencias bancarias con regularidad y tienen proveedores en el extranjero. Esta técnica se lleva a cabo comprometiendo cuentas de correo comerciales legítimas mediante ingeniería social o mediante técnicas de intrusión informática para realizar transferencias no autorizadas normalmente.[5] Según el FBI hay 5 tipos dentro de esta estafa:

  - El CEO Fraud es un tipo de ataque en el que los delincuentes falsifican cuentas de correo electrónico de una empresa para hacerse pasar por ejecutivos y así engañar a empleados de esta empresa, normalmente para que realicen transferencias bancarias no autorizadas o envíen información fiscal confidencial.[6]

    Un ejemplo de este tipo de ataque se dio en 2019 en la sede india de Maire Tecnimont, una empresa italiana de energía e ingeniería. Esta sede recibió un correo electrónico de una cuenta que parecía ser del director ejecutivo de la organización. Este correo solicitaba una transferencia bancaria para una adquisición en China. Se estima que este ataque resultó en unos 18 millones de dólares.[7]

  - El Account Compromise sucede cuando los atacantes hackean la cuenta de correo de un empleado. Utilizan esta cuenta para solicitar pagos de facturas a los proveedores que figuran en sus contactos de correo. Estos pagos son enviados a cuentas bancarias fraudulentas.[6]

  - El Bogus Invoice Scheme es una táctica que utilizan los estafadores que consiste en hacerse pasar por proveedores extranjeros de la empresa normalmente. Estos solicitan transferencias bancarias a cuentas bajo su control.[6]

    En 2019, la parroquia católica de San Ambrose en EEUU fue víctima de este tipo de estafa. Los atacantes se hicieron pasar por proveedores de servicios de la parroquia y reclamaron que no les habían pagado durante meses. Como resultado, consiguieron que párrocos de la iglesia transfiriesen 1,7 millones de dólares a una cuenta fraudulenta.[7]

- El Attorney Impersonation consiste en que los atacantes se hacen pasar por abogados supuestamente a cargo de asuntos cruciales y confidenciales normalmente. Realizan solicitudes falsas por correo electrónico o por teléfono, normalmente al final del horario laboral.[6]
- En el Data Theft, como su nombre indica, el objetivo principal de los atacantes es obtener datos sensibles para luego venderlos o usarlos en futuros ataques. Los empleados que son mayormente objetivo de estos ataques son los de RH y los de contabilidad.[6]

Una vez conocidos los tipos de phishing más relevantes, vamos a observar de qué manera este atañe a la sociedad en general, desde cómo afecta a cada uno de nosotros, hasta su efecto en las empresas, centrándonos principalmente en esta segunda parte.

El atacante emplea diferentes canales para atraer a la víctima mediante una estafa, o de forma indirecta, tipo malware, para obtener información sensible y personal de la víctima. Sin embargo, los ataques de phishing ya han provocado pérdidas perjudiciales y pueden afectar a la víctima, no solo a través de un contexto financiero, sino que también pueden tener otras consecuencias graves como la pérdida de reputación o el compromiso de la seguridad nacional [1].

Aunque estos ataques afectan a las organizaciones y a los individuos por igual, las pérdidas para las organizaciones son más significativas. Una de las principales pérdidas son las económicas del propio ataque, así como el coste asociado a la recuperación, las multas de las leyes/regulaciones de información impuestas por organismos reguladores como HIPAA, PCI y PIPEDA, entre otros. [8]

Este impacto se ha cuadriplicado en los últimos 6 años, con un coste de 14.8 millones de dólares por año para las empresas estadounidenses, comparado con los 3.8 millones en 2015, según el estudio realizado por Ponemon Institute on behalf of Proofpoint [9]. Gastando casi 6 millones de dólares por año en la recuperación tras un ataque de Business Email Compromise (BEC), con 1.17 millones de dólares anuales en pagos ilícitos ejecutados por los atacantes. También el coste de las empresas para proteger sus credenciales ha aumentado considerablemente, de 381.920 dólares en 2015 a 692.531 dólares en 2021.[10]

La estafa de phishing con mayores costes económicos asociados de la historia fue a dos de los gigantes tecnológicos más grandes del mundo, Google y Facebook. Evaldas Rimasauska un hacker lituano, que atacó a ambos entre 2013 y 2015, se hizo pasar por una empresa taiwanesa, Quanta Computer, proveedor de productos electrónicos de ambas empresas. Engañó con éxito a las empresas mediante el envío de facturas falsas que les costó 100 millones de dólares. Finalmente, fue condenado por fraude electrónico y ambas organizaciones, tras trabajar con las autoridades, consiguieron recuperar parte de los fondos. [11]

Otra de los mayores ataques con mayores consecuencias económicas fue en 2016 a Crelan Bank, un banco belga, que perdió 75,8 millones de dólares por culpa de un ataque BEC. Los atacantes comprometieron la cuenta de correo electrónico del director general y engañaron a un empleado para que realizara una transferencia. [11]

Destacar que las consecuencias del phishing para las empresas no son solo costes económicos, otra pérdida aún más importante es la pérdida de datos, ya sea información de los clientes, investigación de proyectos, secretos comerciales o planos. Sobre todo cuando esta empresa se decida a un sector muy competitivo, ya sea industrias farmacéutica, tecnológica o defensa, en las que las pérdidas serían mayores y con un coste mayor de recuperación. [12]

Un ejemplo de ello fue la filtración de información a través del correo electrónico de John Podesta en 2016,

presidente de la campaña electoral de Hillary Clinton. Un grupo de hackers rusos conocido como “Fancy Bear” se hicieron pasar por Google, enviando un correo electrónico diciendo que necesitaba cambiar su correo electrónico después de que ocurriera un intento de pirateo. Tras esto, este grupo obtuvo acceso a su cuenta, llevando a la publicación de miles de correos electrónicos a través de WikiLeaks antes de las elecciones. [13]

Otro coste considerable asociado a estos ataques es la pérdida de productividad de los empleados. Las empresas pierden de promedio 65.343 horas al año debido a ataques de phishing, con un tamaño promedio de 9.567 empleados. Esto es causado por el tiempo que hay que usar en recuperarse del ataque, especialmente en caso de que el ataque haya sido causado por un malware, produciendo que los sistemas deban restaurarse, impidiendo a los empleados realizar sus tareas. [14]

A menudo es habitual que las empresas intenten ocultar los ataques, para evitar daños a su reputación, ya que las divulgaciones públicas de una violación de la seguridad de una empresa pueden contaminarla gravemente, influyendo en la percepción que tienen los clientes, empleados y socios de ella e incluso su pérdida. Esto hace complicado recuperar de nuevo la confianza e influye en el valor de la empresa, dado que este está altamente relacionado con su base de clientes. Un ejemplo de ello es el caso de Facebook, tras un ataque ocurrido en 2018 que puso en compromiso los datos de los usuarios, el valor total de la empresa se redujo en 36 millones de dólares. [12]

También cabe destacar que estos ataques no solo van dirigidos a las grandes empresas, sino que las empresas medianas y pequeñas también son el punto de mira de este tipo de ataques, un estudio efectuado por 2019 Data Breach Investigations Report de Verizon muestra que el 43 % de los ataques son a pequeñas y medianas empresas (pymes) con una tasa de éxito del 63 %. [15]

Hemos visto de una manera un poco general cómo la sociedad, y principalmente las empresas, se ven afectadas por este tipo de ataques cibernéticos. Ahora centraremos algo más el foco y trataremos de ver algunos sectores de la población que se ven más afectados que el resto, así cómo los países y empresas que más ataque reciben, o sectores de trabajadores dentro de una empresa con mayor probabilidad de sufrir un ataque.

2. Segmentos de personas a los que afecta y/o pudiera afectar

Los ciberdelincuentes suelen aprovecharse de los usuarios con falta de conocimiento digital/cibernética o poco formados, además de las vulnerabilidades técnicas para alcanzar sus objetivos. La susceptibilidad al phishing varía entre los individuos según sus atributos y nivel de conciencia, por lo que en la mayoría de los ataques, los phishers explotan la naturaleza humana para hackear, en lugar de utilizar tecnologías sofisticadas. Aunque la debilidad en la cadena de seguridad de la información se atribuye a los humanos más que a la tecnología, no se sabe qué anillo de esta cadena se penetra primero. Los estudios han descubierto que ciertas características personales hacen que algunas personas sean más receptivas a diversos señuelos. Por ejemplo, los individuos que suelen obedecer a las autoridades más que otros son más propensos a ser víctimas de un Business Email Compromise (BEC) que se hace pasar por una institución financiera y solicita una acción inmediata al verlo como un correo legítimo. La codicia es otra debilidad humana que podría ser usada por un atacante, por ejemplo, los correos electrónicos que ofrecen grandes descuentos, tarjetas de regalo gratuitas, y otros. [1]

De forma contradictoria a lo que la mayoría puede pensar, las personas más vulnerables a este tipo de ataque son las personas jóvenes, que en un principio pensaríamos que son las personas que más conocimientos tecnológicos tienen. La Universidad de Carnegie Mellon realizó un estudio en el que envió correos falsos a 515 estudiantes y personal universitario durante 28 días, con el que concluyó que los jóvenes de 18 a 25 años son más susceptibles a caer en la trampa. Esto se puede deber a su menor nivel de experiencia, menor exposición a los materiales de capacitación o la menor concienciación a los riesgos reales. [16] [17]

De forma análoga, las personas mayores y discapacitadas son otro de los segmentos de la sociedad más afectados. Según el informe sobre el fraude a personas mayores del I3 2021, alrededor del 28 % de las pérdidas totales por phishing fueron sufridas por víctimas mayores de 60 años, suponiendo aproximadamente mil millones de dólares en pérdidas para este segmento. [18]

Conforme a un estudio realizado en 2021 sobre email phishing, los hombres son un 225 % más propensos a caer en este tipo de ataque. Sin embargo, esto contradice al estudio ejecutado por Steve Sheng [19] en 2010, sugería que las mujeres eran más susceptibles a este tipo de ataque, en promedio las mujeres hacían click en el correo el 54,7 % y siguiendo dando información una vez clickado el 97 % de las veces. Por ello no podemos concluir de forma clara cuál es el efecto del género de la población a la hora de ser víctimas de este tipo de ataque.

Por otro lado, otro de los principales objetivos de estos ataques son las empresas, viéndose afectadas por igual respecto a los individuos, pero con unas consecuencias de mayor magnitud. Pero dentro del mundo empresarial no todos los sectores se ven afectados de la misma manera ni son atacados por igual.

Según el estudio realizado por Statista Research Department [20] los sectores industriales más afectados son el financiero, Saas (Software como servicio), Comercio electrónico, entre otros. La razón por la que el sector financiero, formado por bancas, seguros, etc. es uno de los más atacados, al igual que el del comercio electrónico, es principalmente porque es de los sectores dónde más capital se mueve, a pesar de también son los que más resistencia y resiliencia cibernética oponen. [21]

De igual manera, no todas las regiones se ven afectadas de la misma forma, en el siguiente estudio se muestra la distribución de las empresas por países que experimentaron un ataque phishing de forma exitosa:

- Estados Unidos: 74 %
- Reino Unido: 66 %
- Australia: 60 %
- Japón: 56 %
- España: 51 %
- Francia: 48 %
- Alemania: 47 %

Por otro lado, la concienciación de la sociedad ante el phishing también varía en función de la región. En este estudio se muestra el porcentaje de población que responde correctamente a la pregunta, ¿Qué es el phishing?

- Reino Unido: 69 %
- Australia: 66 %
- Japón: 66 %
- Alemania: 64 %
- Francia: 63 %
- España: 63 %
- Estados Unidos: 52 %

Como podemos ver según este estudio, no existe una clara relación entre la concienciación sobre el phishing y la susceptibilidad a caer en este engaño, por ello la formación acerca del phishing no es suficiente para prevenir este.[22] [23]

De forma análoga, no todas las empresas se ven afectadas por igual, según un estudio realizado en 2021 por [23] las marcas suplantadas con mayor frecuencia en los ataques phishing son los siguientes:

- Microsoft
- ADP
- Amazon
- Adobe Sign
- Zoom
- Paypal

Dentro de una misma empresa, podemos observar algunos puestos que estarán en la mira de los atacantes y que tendrán más probabilidades de ser objetivo de un ataque de CEO Fraud. Dentro de estos, aparte del CEO, que será el objetivo principal normalmente de estos tipos de ataques, podemos encontrar los siguientes:[24]

- Departamento financiero: Este departamento es especialmente vulnerable en las empresas que realizan regularmente grandes transferencias electrónicas. El director financiero no es el único que puede ser afectado, puede tratarse de cualquier persona de las oficinas de contabilidad que esté autorizada a transferir fondos.
- Recursos humanos: Tiene acceso a todas las personas de la organización, gestiona la base de datos de los empleados y se encarga de la contratación. Como tal, una de sus principales funciones es abrir los currículums de miles de posibles candidatos. Todo lo que necesitan los ciberdelincuentes es incluir un programa espía dentro de un currículum y pueden comenzar a recopilar datos rápidamente de forma encubierta.
- Equipo ejecutivo: Todos los miembros del equipo ejecutivo pueden considerarse un objetivo de alto valor. Muchos poseen algún tipo de autoridad financiera. Si sus cuentas de correo electrónico son hackeadas, generalmente proporciona a los ciberdelincuentes acceso a todo tipo de información confidencial.
- TI: El director de TI y el personal de TI con autoridad sobre los controles de acceso, la gestión de contraseñas y las cuentas de correo electrónico son otros objetivos de gran valor. Si sus credenciales son pirateadas, podrán conseguir entrar en todas las partes de la organización.

Ser conscientes de los sectores de la población más afectados puede ayudar a prevenir el riesgo de phishing, sin embargo si analizamos más detalladamente las características individuales que hacen a las personas más propensas a ser víctimas de este tipo de ataque podremos ser más específicos y precisos a la hora de detectar un potencial sujeto afectado.

3. Signos y/o síntomas (guía de detección / diagnóstico del sujeto afectado)

Ser capaces de comprender y detectar las características que hacen que las personas sean más susceptibles al phishing puede tener una gran utilidad para prevenir este, así como para mejorar las técnicas de

mitigación contra el mismo. Estas características son muy variadas y provienen de diferentes ámbitos, rasgos de personalidad, datos demográficos, experiencia con plataformas, educación… A continuación mencionaremos las que consideramos más relevantes y en las cuales nos basaremos para realizar el test de detección de potenciales víctimas de phishing:[25]

- Agradabilidad: Las personas con un alto grado de simpatía tienen mayor probabilidad de ser víctimas de un ataque.
- Inestabilidad emocional: Aquellos con baja estabilidad emocional son más susceptibles a sufrir un ataque.
- Impulsividad: Cuanto más impulsiva es una persona, mayor es el riesgo de caer en un ataque.
- Búsqueda de sensaciones: Las personas con una mayor búsqueda de experiencias y sentimientos variados, novedosos e intensos son más susceptibles a ser víctimas de un ataque.
- Curiosidad: Los usuarios más curiosos tienen mayor probabilidad de ser víctima de un ataque.
- Sumisión: La obediencia a la autoridad es un predictor significativo de la susceptibilidad al phishing, de modo que aquellos que eran más obedientes eran más susceptibles.
- Edad: Varios estudios han descubierto que la susceptibilidad es mayor para los usuarios de entre 18 y 25 años y disminuye con la edad.
- Nivel de educación. El nivel de educación predijo significativamente la desconfianza hacia el phishing, de tal manera que aquellos con niveles de educación más altos eran más desconfiados, lo que indica que es menos probable que sufran phishing.
- Conocimientos de phishing: Los que están familiarizados con la definición de phishing son significativamente menos propensos a caer en el.
- Alfabetización informática: La autoeficacia de un usuario al utilizar un ordenador es un predictor muy importante de la susceptibilidad al phishing, de modo que los que tenían una mayor alfabetización eran menos susceptibles.
- Uso habitual: El uso habitual de las plataformas, o los patrones de comportamiento fijos y repetidos al interactuar con una plataforma, provocan falta de atención y una menor implicación consciente. El uso habitual del correo electrónico contribuye significativamente a la susceptibilidad al phishing
- Adicción a internet: Es un predictor positivo significativo de los comportamientos de riesgo en ciberseguridad relacionados con caer en un ataque de phishing.
- Tendencia a leer completamente los correos electrónicos. Los usuarios que leen completamente los correos electrónicos son significativamente mejores en la detección de correos electrónicos de phishing.

Por ello, tomando estas características, procedemos a realizar un estudio que nos ayude a detectar el riesgo de caer en un ataque de phishing en la medida de lo posible, basándonos en las siguientes cuestiones:

- Pregunta: 1.¿Cuál es tu edad? Respuestas:-18…18-25….26-45…..46-60…..+60
- Pregunta: 2.¿Cuál es tu nivel de estudios superado? Respuestas: Infantil y primaria—-ESO—-Bachiller/Grado medio——Grado universitario/Grado superior—-Estudios superiores
- Pregunta: 3. ¿Cómo de frecuentemente utilizas el correo electrónico? Respuestas:Menos de una vez a la semana—-Menos de una vez al día—Pocas veces al día——Una vez al día—-Varias veces al día

- Pregunta: 4.¿Cómo de agradable con la gente te consideras? Respuestas: poco 1-5 mucho
- Pregunta: 5.¿Cómo de inestable emocionalmente te consideras? Respuestas: poco 1-5 mucho
- Pregunta: 6.¿Cómo de impulsivo te consideras? Respuestas: poco 1-5 mucho
- Pregunta: 7.¿Te consideras una persona que busca nuevas experiencias y sensaciones novedosas e intensas a menudo? Respuestas: poco 1-5 mucho
- Pregunta: 8.¿Cómo de curioso te consideras? Respuestas: poco 1-5 mucho
- Pregunta: 9.¿Te consideras una persona sumisa y obediente frente a la autoridad? Respuestas: poco 1-5 mucho
- Pregunta: 10. ¿Cómo de familiarizado con el phishing consideras que estás? Respuestas: poco 1-5 mucho
- Pregunta: 11. ¿Cuál consideras que es tu nivel de alfabetización informática? Respuestas: poco 1-5 mucho
- Pregunta: 12. ¿Cómo de alta consideras que es tu adicción a internet? Respuestas: Muy baja 1-5 muy alta
- Pregunta: 13. ¿Lees los correos que recibes completamente? Respuestas: Siempre—Casi siempre—-A veces—-Casi nunca——Nunca
- Pregunta: 14. Como miembro de una empresa recibes un correo electrónico de parte de los técnicos de la misma que contiene un enlace a una página web en la que te solicitan tus credenciales de correo de empresa para poder acceder a una información para un nuevo proyecto que acabas de empezar. Esta información no ha sido solicitada por tu parte. ¿Consideras que este caso real es un caso de phishing? Respuestas: Sí/No
- Pregunta: 15. Como parte del departamento de finanzas de tu empresa recibes un correo electrónico del CEO de la misma solicitando la realización de una transferencia bancaria a un proveedor extranjero nuevo. Solicita que esta transferencia se haga con urgencia para cerrar la compra cuanto antes. La suma de dinero de esta transferencia no es una cifra relevante para la empresa. ¿Consideras que este caso real es un caso de phishing? Respuestas:Sí/No
- Pregunta: 16. Como desarrollador en una empresa recibes un correo que contiene un archivo .zip en el que te indican que está el proyecto de una nueva aplicación. Como jefe de ese proyecto te solicitan que compruebes la calidad del software, para lo que debes descargar este archivo en tu máquina local y descomprimirlo. ¿Consideras que este caso real es un caso de phishing? Respuestas: Sí/No
- Pregunta: 17. Recibes un correo de Dropbox en tu correo de empresa indicando que el almacenamiento de tu cuenta está a punto de llenarse y necesitas actualizar tu plan de suscripción. Para actualizarlo aparece un enlace en el correo que te lleva a la página oficial de Dropbox en la que ya tienes iniciada sesión. ¿Consideras que este caso real es un caso de phishing? Respuestas: Sí/No
- Pregunta: 18. Desde la cuenta no-reply@google.support recibes un correo electrónico indicando que es posible que atacantes respaldados por un gobierno estén intentando robar tu contraseña. En el correo aparece un enlace para cambiarla. La URL de este enlace es el siguiente: www.gooogle.es/cambio-contraseña. ¿Consideras que este caso real es un caso de phishing? Respuestas: Sí/No
- Pregunta: 19. Recibes un mensaje desde el mismo número de teléfono/conversación de la que te llegan los mensajes de los bizums, pagos que realizas, etc, de tu banco informándote de que ha habido un pago no autorizado y que para cancelarlo tienes que acceder con tus credenciales al enlace adjunto que te dirige a una página similar a la de tu banco, pero que solo te deja iniciar sesión con tus credenciales. ¿Consideras que este caso real es un caso de phishing? Respuestas: Sí/No

Las 13 primeras preguntas de este cuestionario sirven para observar las características de la persona y así poder darle una puntuación del 1 al 10 a la susceptibilidad de este usuario para caer en un ataque de phishing. Las 6 preguntas restantes son casos reales que se le proponen al usuario, dejando pequeñas pistas sobre si es un ataque de phishing o no, para ver si este realmente caería o no en una estafa de phishing. De estas 6, la única que no es un caso de estafa es la número 17. Para obtener la puntuación de susceptibilidad al phishing se les dan las siguientes puntuaciones a cada respuesta:

- Pregunta 1: Respuesta 1 suma 3 puntos. Respuesta 2 suma 4 puntos. Respuesta 3 suma 0 puntos. Respuesta 4 suma 1 punto. Respuesta 5 suma 2 puntos.
- Pregunta 2: Respuesta 1 suma 4 puntos. Respuesta 2 suma 3 puntos. Respuesta 3 suma 2 puntos. Respuesta 4 suma 1 punto. Respuesta 5 suma 0 puntos.
- Pregunta 3: Respuesta 1 suma 0 puntos. Respuesta 2 suma 1 punto. Respuesta 3 suma 2 puntos. Respuesta 4 suma 3 puntos. Respuesta 5 suma 4 puntos.
- Preguntas 4 a 13: Sus respuestas van en una escala de 1 a 5. Cada respuesta suma su número menos 1.

Todos estos signos son muy fáciles de detectar sobre el papel, pero cuando ponemos en estas situaciones a los empleados de una organización hay ciertos riesgos de caer en ellos. Para comprobar la toma de conciencia y la detección de estos riesgos es de gran interés el cuestionario realizado por Jigsaw de Google [26] que abarca diferentes ataques descritos anteriormente y simula como si fuera la realidad de los diferentes mensajes y permite una pequeña interacción con ellos(8 casos reales en los que te indicará en qué parte del mensaje puedes identificar si es un intento de phishing o no).

El por qué de la creación de nuestro propio cuestionario frente al de Jigsaw se debe basicamente el poder acceder a los datos del usuario y poder hacer las preguntas de control de características que nos permiten poder hacer un mejor estudio posterior, además que para la difusión del experimento/cuestionario resultaba más comodo para los encuestados tener agrupado en un solo enlace las preguntas y los casos reales. Sin embargo, podemos ver su utilización en el TFG *"Análisis y Simulación de un Ataque de Phishing"* [27] y sus conclusiones acerca de los datos extraidos.

Se ha identificado que la edad, el conocimiento tecnológico, la adicción a Internet, el estrés del usuario y muchos otros atributos afectan a la susceptibilidad al phishing entre las personas. Pero esto son solo factores que nos indican una predisposición a poder caer en el phishing. Todavía no existe una solución única en la que se pueda confiar o que sea capaz de mitigar estos ataques. Incluso identificando los riesgos, hay un gran trecho entre el papel y la realidad, por lo que hay que trabajar en desarrollar algunas estrategias para actuar contra este riesgo.

4. Estrategias contra este riesgo (guía de actuación)

Para contar con una guía de actuación frente al phishing comenzaremos mencionando medidas que ayudarán a prevenir este riesgo todo lo posible, a continuación hablaremos sobre medidas de paliación para poder contenerlo y evitar en gran parte sus efectos, y por último, si ha sucedido, medidas de acción [8] [28] [29].

4.1. Planes de prevención

Realizar una formación periódica de concienciación sobre el phishing y su reconocimiento

Según los expertos, el coste producido por los ataques phishing se puede reducir hasta en un 50 % con un entrenamiento de concienciación de seguridad frente a este. Esto hace que el correo electrónico sea un objetivo principal para los atacantes. Una de las formas más eficaces de prevenir los ataques de phishing es llevar a cabo una formación periódica sobre ciberseguridad para todos los empleados de la organización.

La formación sobre el phishing ayudará a sus empleados a reconocer las diversas tácticas que emplean los atacantes para engañarles y hacer que proporcionen información sensible. También se asegurará de que sepan a qué deben prestar atención y les hará comprender la importancia de denunciar estas situaciones con la suficiente antelación. El aspecto de la periodicidad también es clave en este aspecto, para poder mantener informados a los usuarios/empleados sobre los últimos ataques de phishing y sus identificadores clave

No proporcione su información a sitios web no seguros

Si la URL de la web no comienza con https o si no ve un icono de candado cerrado junto a la URL, no ingrese información confidencial ni descargue archivos del sitio.Los usuarios deben asegurarse, si tienen que dar información acerca de algo importante, que el sitio web es auténtico, que la empresa es real y que el propio sitio sea seguro.

Cambiar las contraseñas regularmente

La cuenta de los usuarios podría verse comprometida sin su conocimiento, por lo que agregar una capa adicional de protección a través de la rotación/cambio de contraseñas puede prevenir ataques continuos y disuadir a posibles atacantes. El uso de autenticación multifactorial y/o de doble factor también ayuda a poner algo más complicado a los atacantes su objetivo.

No hagas clic en ese enlace

Ciertos ataques de phishing son tan sofisticados que la URL de destino puede parecer una copia del sitio web real, configurada para robar información de inicio de sesión o incluso, de tarjetas de crédito. Antes de hacer clic en un link del correo electrónico, el usuario debería revisar si la página a la que le redirigirá es legítima y del objetivo del remitente del correo electrónico.

No ignorar las actualizaciones

Si los usuarios no realizan las actualizaciones propuestas corren el riesgo de sufrir ataques de phishing a través de vulnerabilidades conocidas que podrían haberse evitado. Estas actualizaciones se encuentran al día con los métodos modernos de ciberataque, parcheando agujeros en la seguridad.

Instalar cortafuegos y software antiphishing

Tanto los cortafuegos de escritorio como los cortafuegos de red, una vez que se aplican conjuntamente, tienen la posibilidad de reforzar su estabilidad y minimizar las posibilidades de que un hacker se infiltre en su entorno. El software antiphishing también permite detectar enlaces dañinos y anticiparse a un ataque dirigiendo al usuario en las direcciones correctas.

No dar información importante a menos que debas hacerlo Los usuarios deben asegurarse, si tienen que

dar información acerca de algo importante, que el sitio web es auténtico, que la empresa es real y que el propio sitio sea seguro.

Disponer de una plataforma de seguridad de datos para detectar los signos de un ataque

Si un usuario ha sido víctima de un ataque de phishing, es importante que sea capaz de detectar y reaccionar a tiempo, siguiendo alguno de los pasos que se comentan en el punto 4.3. Sin embargo, si se cuenta con una plataforma de seguridad de datos, será posible aliviar la tensión del equipo de TI/Seguridad, debido a que se alerta de manera automática sobre comportamientos anómalos. Esto puede ayudar también a identificar cuentas afectadas y favorecer a tomar medidas para evitar más daños.

Estilo del mensaje

Una señal rápida de phishing es que un mensaje esté compuesto con un lenguaje o tono indebido. Si, por ejemplo, un compañero de trabajo suena excesivamente relajado, o un compañero querido utiliza un lenguaje formal, esto debería provocar dudas. Los destinatarios del mensaje deberían comprobar si hay algo más que pueda indicar que se trata de un mensaje de phishing.

Errores lingüísticos

Los errores lingüísticos y la ortografía incorrecta son otros signos de los mensajes de phishing.La mayoría de las organizaciones han introducido el corrector ortográfico en sus programas de correo electrónico, por lo tanto, los mensajes con errores ortográficos o lingüísticos deberían despertar alertas, ya que probablemente no provienen de la fuente que se está reconociendo.

Peticiones peculiares

Podría ser un indicio de que un correo electrónico es inseguro en el caso de que exija una forma extraña de comportarse por su parte. Por ejemplo, si un correo electrónico exige la descarga de un programa y da a entender que procede de un grupo de TI concreto, mientras que en realidad la división de TI suele encargarse de estas tareas, lo más seguro es que el correo electrónico sea falso.

Archivos adjuntos sospechosos

Si se recibe un correo electrónico con un archivo adjunto de una fuente desconocida, o si el destinatario no solicitó ni esperaba recibir un archivo del remitente del correo electrónico, el archivo adjunto debe abrirse con precaución. Si el archivo adjunto tiene una extensión comúnmente asociada a las descargas de malware (.zip, .exe, .scr, etc.) -o tiene una extensión desconocida- los destinatarios deben marcar el archivo para que sea analizado por un antivirus antes de abrirlo.

El destinatario no inició la conversación

Dado que los correos electrónicos de phishing no son solicitados, un gancho que se utiliza a menudo es informar al destinatario de que ha ganado un premio, de que tendrá derecho a un premio si responde al correo electrónico o de que se beneficiará de un descuento si hace clic en un enlace o abre un archivo adjunto. En los casos en que el destinatario no haya iniciado la conversación optando por recibir material de marketing o boletines informativos, hay una alta probabilidad de que el correo electrónico sea sospechoso.

Variedades en las direcciones web

La búsqueda de direcciones de correo electrónico, URL y nombres de área mezclados es otra estrategia

sencilla para reconocer probables ataques de phishing. Comprobar un mensaje anterior que coincida con la dirección de correo electrónico de la fuente es un aspecto a observar.

Antes de hacer clic en un link del correo electrónico, el usuario debería revisar si la página a la que le redirigirá es legítima y del objetivo del remitente del correo electrónico. Cuando un correo electrónico parece provenir del Banco Santander, pero el espacio de la dirección de correo electrónico no contiene "bancosantander.es", es probable que se trate de un correo electrónico de phishing.

Interés por la identificación, el pago u otra información personal

Los agresores utilizan habitualmente mensajes que parecen legítimos para conectar con falsos locales de inicio de sesión que parecen auténticos. En la página de inicio de sesión falsa se puede encontrar un cuadro de inicio de sesión o una solicitud de datos bancarios. El beneficiario no debería tocar la conexión o introducir sus datos de acceso en caso de que no haya solicitado el correo electrónico. Los beneficiarios deberían ir rápidamente al sitio oficial que aceptan como remitente del correo electrónico como medida de seguridad.

4.2. Planes paliativos / contención

La identificación de alguno de estos riesgos comentados anteriormente es el primer paso en la batalla contra los "phishers". Sin embargo, lo más probable es que si un empleado está recibiendo correos electrónicos de phishing, otros también lo estén.Las organizaciones deben promover prácticas para que los empleados informen en este tipo de casos: "Si ves algo, di algo", para alertar a la seguridad o al equipo de respuesta a incidentes.

Del mismo modo un usuario que haya sido atacado con éxito, no debe alarmarse y debe mantener la calma ya que existen ciertas medidas que pueden seguir para salvaguardar su información comprometida [30]:

Desconectar el dispositivo

Si se ha cometido el error de descargar un malware o se visitó un enlace de phishing, lo primero que debe hacer el usuario es cortar la conexión a Internet del dispositivo. Es importante hacerlo de inmediato para reducir el riesgo de que el malware se propague a otros dispositivos de la red.

Hacer una copia de seguridad

Una vez el usuario se haya desconectado de la red, debería proceder a realizar una copia de seguridad de los archivos más preciados y documentos sensibles, debido a que es posible perder los datos en el proceso de recuperación del ataque de phishing.

Cambiar las credenciales

En el caso de haber entrado en un enlace malicioso que haya dirigido al usuario a un sitio web falso, este debería cambiar su nombre de usuario y contraseña inmediatamente. Cabe recordar que no se debería utilizar el mismo nombre de usuario y contraseña para todas las cuentas que se tengan online, ya que esto facilita al atacante robar su identidad y acceder a sus fondos.

Escanear el sistema en busca de malware

Esta tarea no tiene mucha dificultad, únicamente debe asegurarse de utilizar un servicio de confianza para

garantizar que el problema se resuelva de forma segura.

4.3. Planes de acción

En este caso, los usuarios deberían comprobar quién, qué, cuándo y dónde ocurrió el incidente en cuestión. Para ello, deberían seguir algunas de las medidas que se comentan a continuación [31] [32]:

Reportar el incidente y cambiar credenciales

En el momento que nos demos cuenta que hemos sido víctimas del ataque deberíamos reportar a las autoridades y al remitente oficial el cuál han suplantado (tu banco, el departamento de tu empresa...) ya que posiblemente tenga protocolos para gestionar este tipo de situaciones tan recurrentes en el día a día.También deberías cambiar las credenciales de todas las cuentas que utilizan la misma contraseña.

Uso de antivirus y antimalware

Es posible que se hayan abierto puertas traseras para un troyano o spyware, al haber sido víctima de una estafa de phishing. Por ello, los usuarios deberían ejecutar un análisis completo y eliminar cualquier archivo sospechoso.

Mantenerse actualizado

Como usuarios afectados, deben aprender de los errores y mantenerse actualizados sobre las nuevas estafas que haya por Internet. Si necesitase ayuda para implementar estos pasos, no dudar en contactar con un técnico especializado.

Proteger cuentas e información personal para evitar caer de nuevo en estafas de Internet

Para casos futuros, revisar con cuidado las bandejas de entrada y examinar cuidadosamente los enlaces o archivos que pudiesen ser sospechosos. A la hora de revelar cualquier información personal, es mejor ir directamente al sitio web para iniciar sesión o ponerse en contacto con la empresa para verificar que los correos recibidos son legítimos.

Referencias

[1] A. Zainab, H. Chaminda, N. Liqaa and K.Imtiaz.“Phishing Attacks: A Recent Comprehensive Study and a New Anatomy”, Frontiers in Computer Science, vol.3, pp.1-23, March 2021.

[2] Panda Security. (2021, April 12). 11 Types of Phishing + Real-Life Examples (1st ed.) [Online]. Available: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/ Last access: 2022-03-10

[3] Fortinet. 19 Types of Phishing Attacks with Examples (1st ed.) [Online]. Available: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks Last access: 2022-27-09

[4] J. Fruhlinger. (2022, April 07). What is spear phishing? Examples, tactics, and techniques (1st ed.) [Online]. Available: https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html Last access: 2022-27-09

[5] Gatefy. (2021, March 18). What is BEC (Business Email Compromise) or CEO Fraud? (2nd ed.) [Online]. Available: https://gatefy.com/blog/what-bec-business-email-compromise-or-ceo-fraud/ Last access: 2022-28-09

[6] Trend Micro. Business Email Compromise (BEC) (1st ed.) [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec) Last access: 2022-28-09

[7] Gatefy. (2021, June 28). 10 real and famous cases of BEC (Business Email Compromise) (2nd ed.) [Online]. Available: https://gatefy.com/blog/real-famous-cases-bec-business-email-compromise/ Last access: 2022-28-09

[8] Wallarm Blog. Types Of Phishing Attacks And Business Impact [Online]. Available: https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact Last access: 2022-26-09

[9] Ponemon Institute, ”The Ponemon 2021 Cost of Phishing Study”, vol. 1, pp 39, June 2021.

[10] D. Jones. (2021, August 17). How much does phishing really cost the enterprise?. [Online]. Avaible: https://www.cybersecuritydive.com/news/phishing-cost-enterprise/605110/ Last Access: 2022-27-09

[11] A. Purohit. (2021, July 15). 5 of the most expensive phishing scams in history. [Online]. Avaible: https://www.delta-net.com/blog/5-of-the-most-expensive-phishing-scams-in-history/ Last access: 2022-29-09

[12] PacketLabs. (2020, October 15). What is the business impact of a Phishing Attack?. [Online]. Avaible: https://www.packetlabs.net/posts/impact-of-phishing-attack/. Last access: 2022-26-09

[13] R. Vidwans. 5 Biggest Data Breaches of All Time from Phishing. [Online]. Available: https://www.clearedin.com/blog/phishing-biggest-data-breaches-of-all-time. Last access: 2022-28-09

[14] C. Sánchez. (2021, August 19). El coste medio del phishing se ha casi cuadruplicado desde 2015. [Online]. Available: https://cybersecuritynews.es/el-coste-medio-del-phishing-se-ha-cuadruplicado-desde-2015/. Last access: 2022-28-09.

[15] Verizon, (2022, May 24). 2022 Data Breach Investigations Report. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. Last access: 2022-01-10.

[16] Redaccion EnigmaSoft. Un Estudio Muestra que los Jóvenes Usuarios de Internet Son Más Vulnerables a los Ataques Phishing. [Online]. Avaible: https://www.enigmasoftware.es/estudio-muestra-jovenes-usuarios-internet-mas-vulnerables-ataques-phishing/. Last access: 2022-10-03.

[17] A. Rahman. (2022, May 19). Phishing Report 2022: Which Individuals Are Most at Risk. [Online]. Avaible: https://secureteam.co.uk/articles/phishing-report-2022-which-individuals-are-most-at-risk/. Last access: 2022-10-03.

[18] Redaccion Computing. (2022, January 03). 22 estadísticas de ciberseguridad que hay que conocer para 2022. [Online]. Avaible: https://www.computing.es/seguridad/informes/1130465002501/22-estadisticas-de-ciberseguridad-hay-conocer-2022.1.html. Last access: 2022-10-03.

[19] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, J. Downs, ”Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions”, vol. 1, 373–382, April 2010.

[20] Statista Research Department. (2022, July 2022). Phishing: most targeted industry sectors 2022. [Online]. Avaible: https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/. Last Access: 2022-10-04.

[21] D. Brecht. (2016, May 20). Phishing Attacks by Demographic. [Online]. Avaible: https://resources.infosecinstitute.com/topic/phishing-attacks-by-demographic/. Last Access: 2022-10-04.

[22] Proofpoint, ”State of the Phish”, vol. 1, March 2022.

[23] M. Rosenthal. (2022, January 12). Must-Know Phishing Statistics: Updated 2022. [Online]. Avaible: https://www.tessian.com/blog/phishing-statistics-2020/. Last access: 2022-10-03.

[24] KnowBe4. CEO Fraud & Executive Phishing Email Attacks | KnowBe4 (2nd ed.) [Online]. Available: https://www.knowbe4.com/ceo-fraud Last access: 2022-04-10.

[25] K. Tornblad, K. Jones, A. Siami and J. Choi, Çharacteristics that Predict Phishing Susceptibility: A Review”, in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2021, pp. 938–942.

[26] *Phishing Quiz*. Jigsaw - Google. Available: https://phishingquiz.withgoogle.com/ Last access: 2022-01-10

[27] V. Barroso Beltri, “Análisis y Simulación de un Ataque de Phishing” Treball Final de Grau, UPC, Facultat d’Informàtica de Barcelona, Departament d’Arquitectura de Computadors, 2021.

[28] Cyberint Blog.(2022, March 28). Five Steps to Protect Your Organization against Phishing Attacks [Online]. Available: https://cyberint.com/blog/thought-leadership/phishing-protection-guide/ Last access: 2022-26-09

[29] A.Simister.(2022, September 14). 10 Ways to Prevent Phishing Attacks [Online]. Available: https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/ Last access: 2022-26-09

[30] Eloan Blog. 7 Steps to Take Now If You’re a Victim of a Phishing Attack [Online]. Available: https://www.eloan.com/blog/personal-finance/7-steps-to-take-now-if-youre-a-victim-of-a-phishing-attack Last access: 2022-27-09

[31] L. Díaz Moreno (2021, Noviembre 18). He caído en un ‘phishing’ o estafa de internet: ¿qué puedo hacer? Te damos 6 recomendaciones clave [Online]. Available: https://www.newtral.es/phishing-que-hacer-victima-estafa/20211118/ Last access: 2022-27-09

[32] Mental Floss Editorial (2017, August 3). 7 Steps to Take Now if You’re the Victim of a Phishing Scheme [Online]. Available: https://www.mentalfloss.com/article/503105/7-steps-take-now-if-youre-victim-phishing-scheme Last access: 2022-27-09

Anexo: Estudio de campo

Tras difundir la encuesta diseñada que en el punto 3 llegamos a obterner unas 149 respuestas. Estas abarcaron diferentes rangos de población, con una mayor predominancia por el de 18-25, ya que es el grupo de edad de los integrantes de este grupo.

Sin embargo podemos hacer un análisis de los datos que nos permitan ver si las cualidades que hemos identificado, vemos su correlación en el estudio realizado.

Si profundizamos en los casos reales planteados, podemos ver lo siguiente:

- Caso 1: Este caso fue planteado como un ataque de phishing. Los resultados que nos vuelca la encuesta es que el 78.2 % de los encuestados han acertado.
- Caso 2: También este caso formaba parte de los casos de phishing que queríamos comprobar en los encuestados. El 74.1 % de estos acertaron.
- Caso 3: Este caso era otro de phishing. En este sin embargo los resultados estuvieron más ajustados, y solo el 58.5 % de los encuestados han acertado.
- Caso 4: Este es el único caso que no se trataba de phishing, y al igual que el anterior solo el 59.2 % acertaron.
- Caso 5: El caso 5 se trataba de un tipo de phishing (había que darse cuenta de la URL) y en acertaron el 77.6 % de los encuestados.
- Caso 6: El último también se trataba de un caso de phishing (este quizá la descripción fue más clara para identificarlo) y este fue en el que los encuestados acertaron en mayor medida (88.4 %).

Como vemos hay un cierto porcentaje de la población que caería en 1 o más casos de este tipo planteados en el cuestionario (y seguramente en la realidad en mayor medida ya que la descripción propuesta ayudaba en gran parte a identificar si era o no phishing).

Para ello y tomando las respuestas al cuestionario , planteamos las puntuaciones comentadas para el experimento 3. Tras esto , vemos cuantos fallos en la detección de los casos reales planteados han realizado los encuestados.

Num fallos	Respuestas
0	23
1	62
2	26
3	24
4	12
5	2
6	0

Cuadro 1: Tabla distribución número fallos.

Gráficamente podemos observar en un box plot la distribución de estos para poder sacar unas mejores conclusiones. En el gráfico se representan la puntuación de cada uno de los individuos según sus respuestas a las preguntas de sus características y su distribución respecto a los fallos en los casos propuestos.

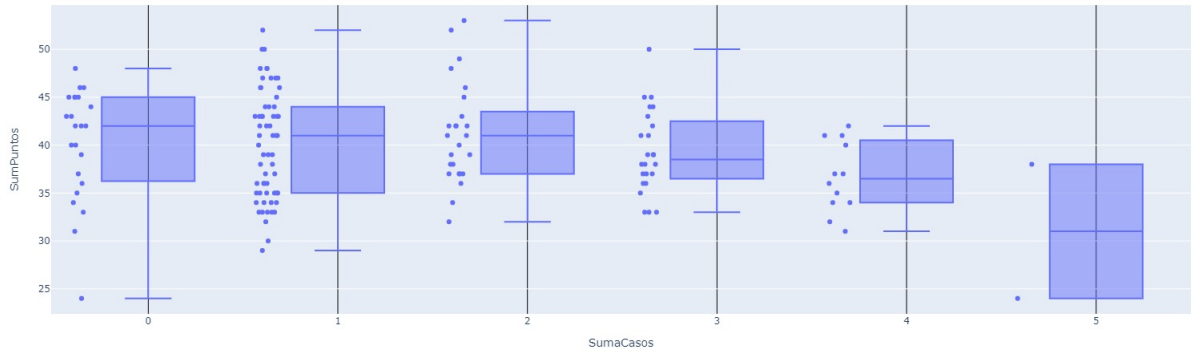


Figura 1: Análisis box plot puntuación-características respecto al número de fallos.

Se puede observar cómo se distribuyen un mayor número de puntos en torno a los 1-2 fallos en los casos. Más concretamente en las características vemos cómo por debajo de los 32 puntos existen pocas personas que hayan fallado, datos acordes a lo esperado en la tesis planteada. También podemos observar cómo entre los 35 y 45 puntos en características están concentradas la mayoría de las personas.

Sin embargo, la distribución de los fallos y su correlación con la puntuación en las características es algo heterogénea, es decir, no solo dependen de una característica, ni todas las características en su conjunto nos hacen más predispuestos a caer en un ataque de phishing. Por esto podemos ver cómo en un cierto grado las características de las personas pueden influir en su susceptibilidad para caer en un ataque, pero sin darnos una gran certeza sobre ello.

Por eso es de gran importancia que los usuarios reciban formación y estén al tanto de los últimos casos de phishing, y que aparte de su identificación, sepan cómo actuar ante estos y seguir manteniéndose seguros ante tales amenazas. También cabe destacar que no solo los usuarios son los que deben actuar para tratar de paliar el phishing, sino que las empresas también juegan un papel clave.

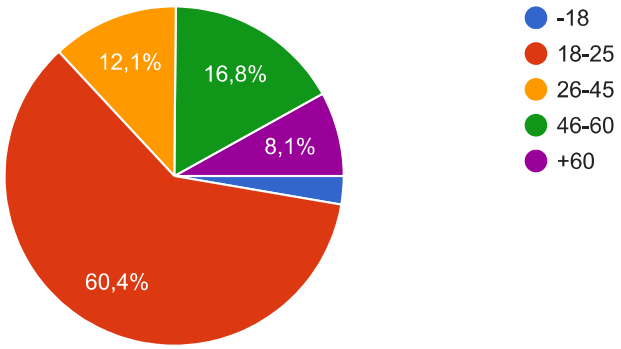
Phishing

149 respuestas

¿Cuál es tu edad?

Copiar

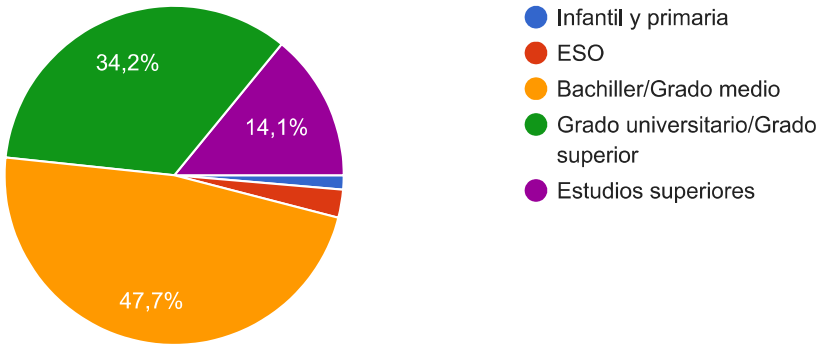
149 respuestas



¿Cuál es tu nivel de educación superados?

Copiar

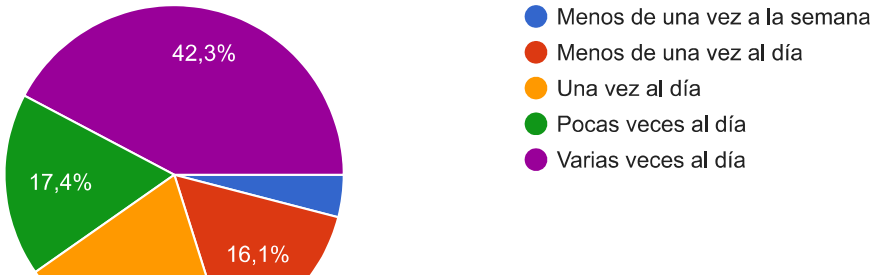
149 respuestas

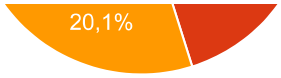


¿Cómo de frecuentemente utilizas el correo electrónico?

Copiar

149 respuestas

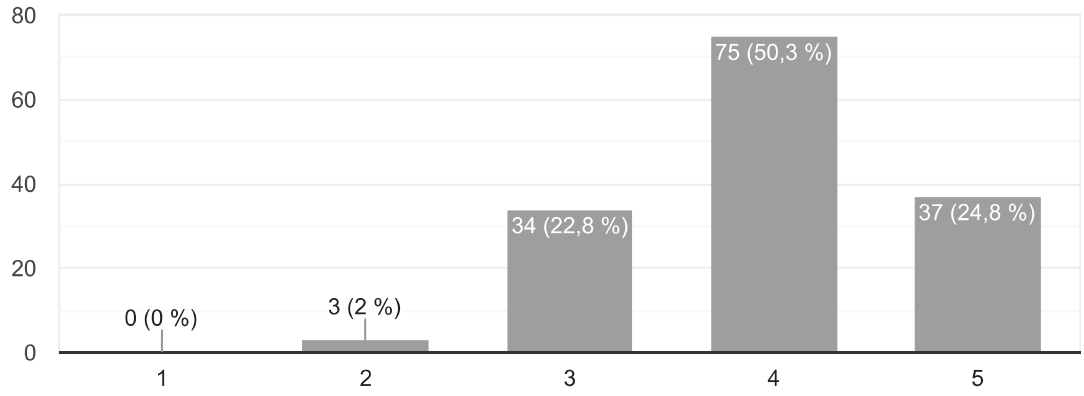




Copiar

¿Cómo de agradable con la gente te consideras?

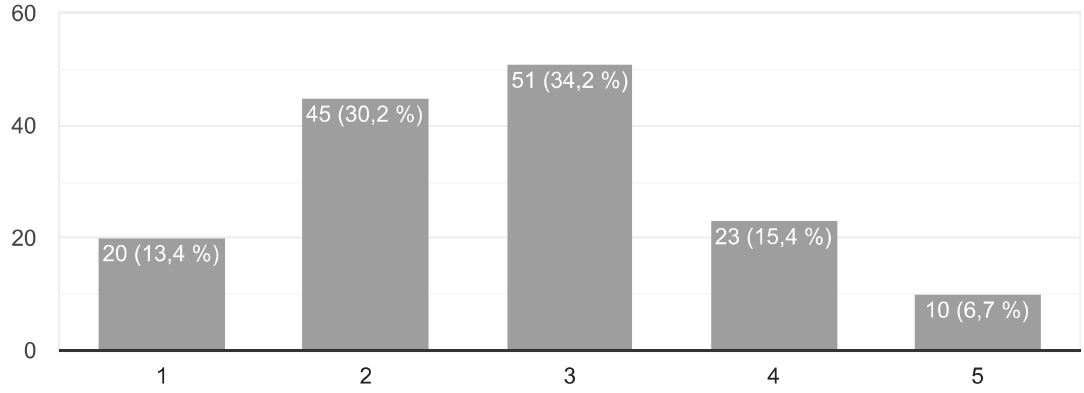
149 respuestas



Copiar

¿Cómo de inestable emocionalmente te consideras?

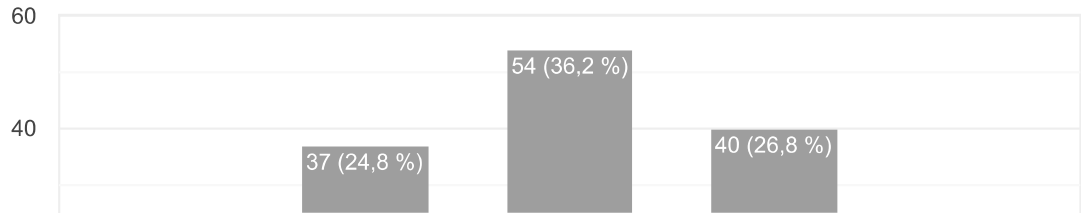
149 respuestas

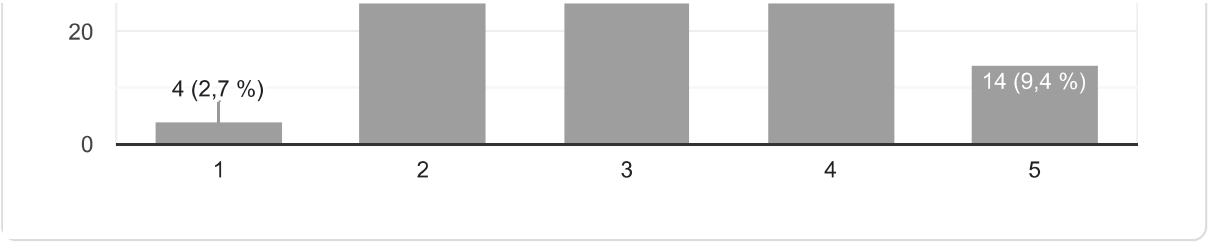


Copiar

¿Cómo de impulsivo te consideras?

149 respuestas

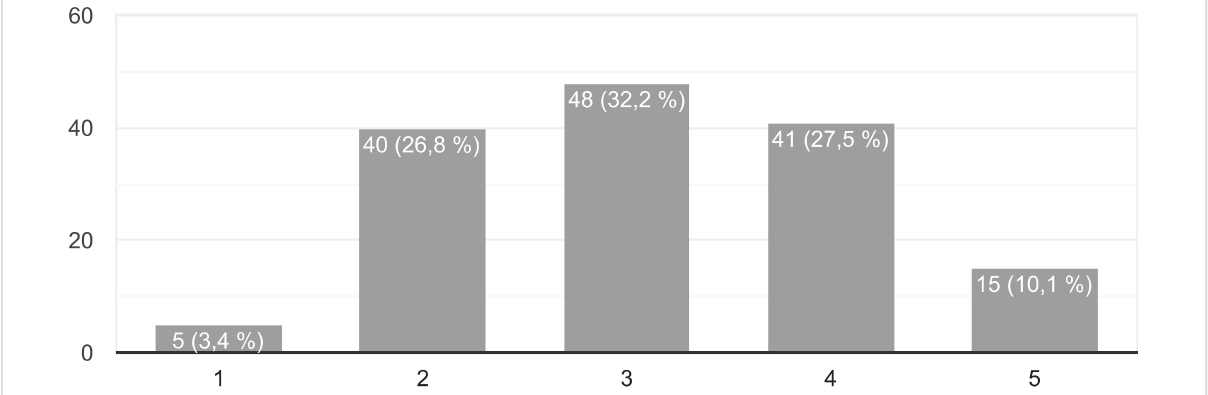




¿Te consideras una persona que busca nuevas experiencias y sensaciones novedosas e intensas a menudo?

Copiar

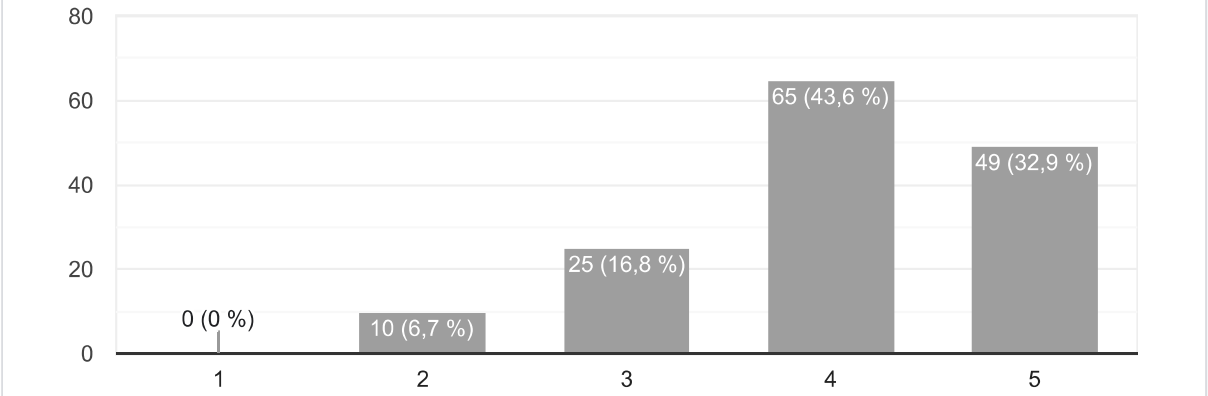
149 respuestas



¿Cómo de curioso te consideras?

Copiar

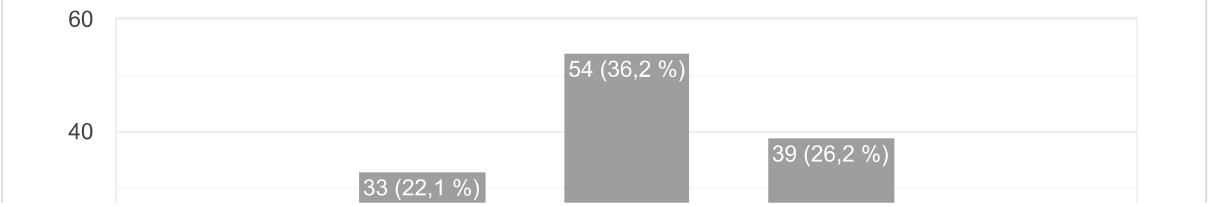
149 respuestas

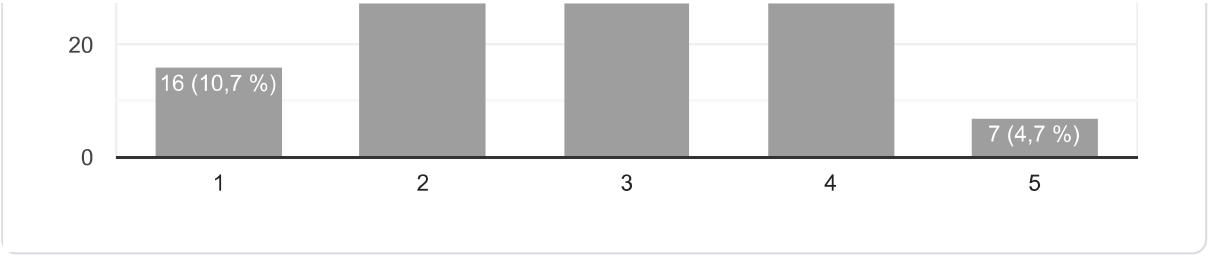


¿Te consideras una persona sumisa y obediente frente a la autoridad?

Copiar

149 respuestas

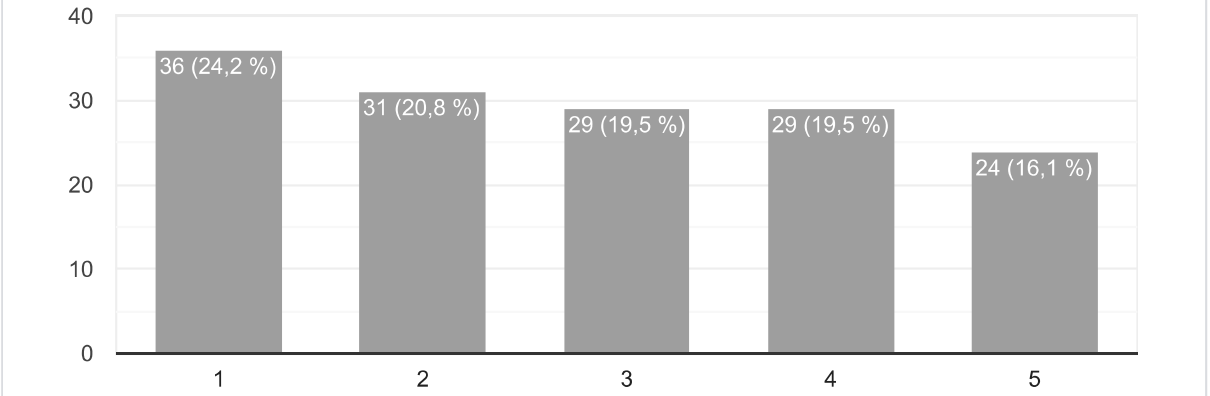




¿Cómo de familiarizado con el phishing consideras que estás?

Copiar

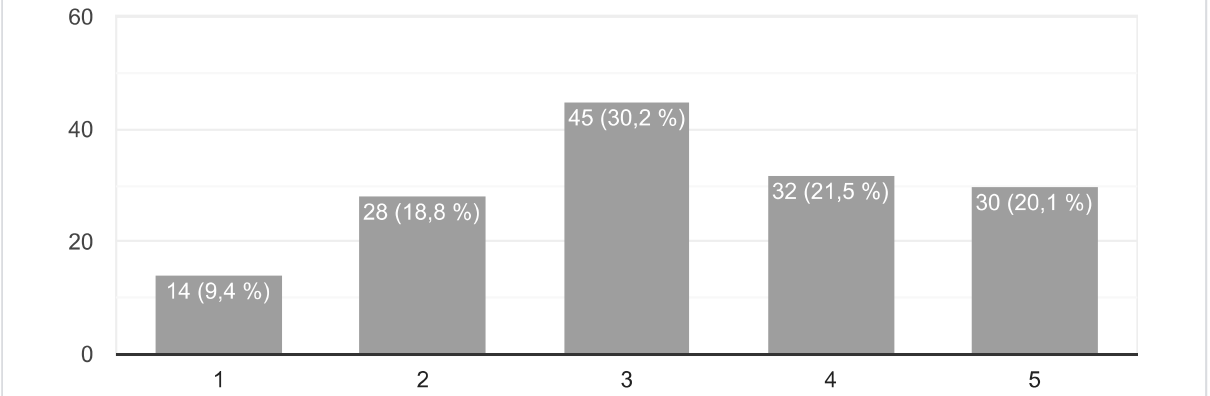
149 respuestas



¿Cuál consideras que es tu nivel de alfabetización informática?

Copiar

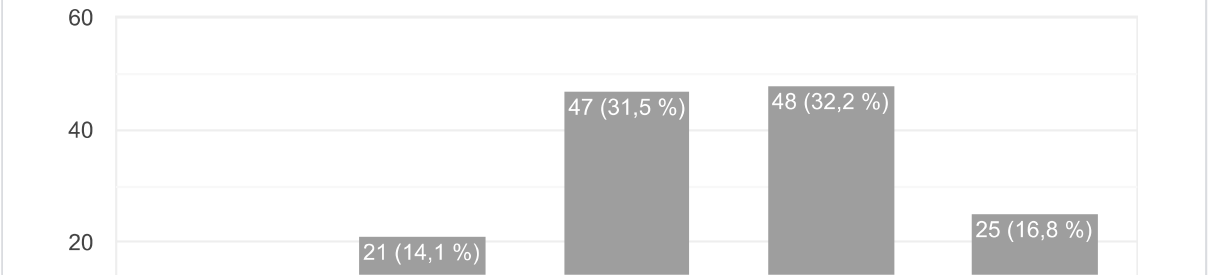
149 respuestas

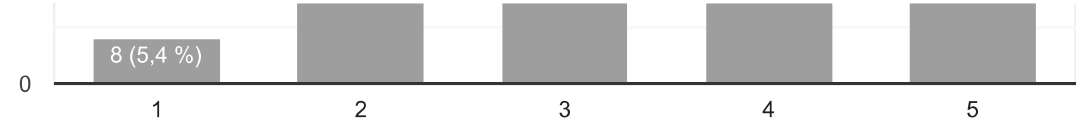


¿Cómo de alta consideras que es tu adicción a Internet?

Copiar

149 respuestas

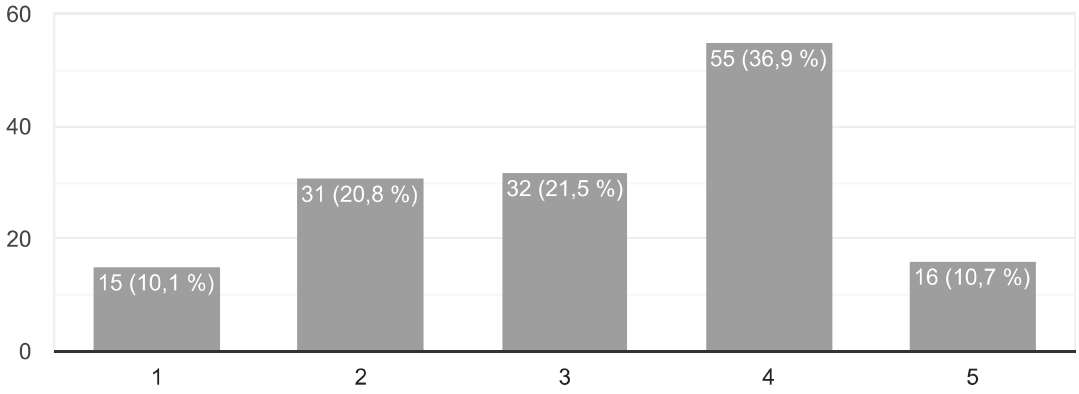




¿Lees completamente los correos que recibes?

Copiar

149 respuestas



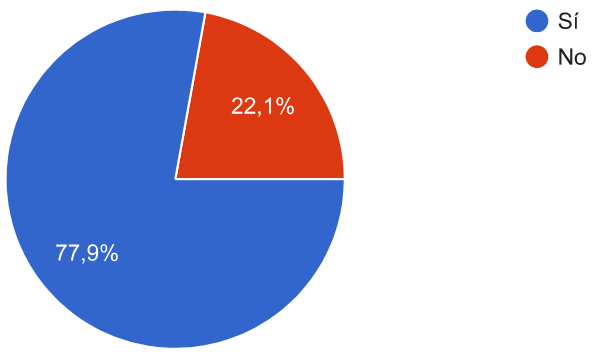
Casos reales

Como miembro de una empresa recibes un correo electrónico de parte de los técnicos de la misma que contiene un enlace a una página web en la que te solicitan tus credenciales de correo de empresa para poder acceder a una información para un nuevo proyecto que acabas de empezar. Esta información no ha sido solicitada por tu parte.

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas

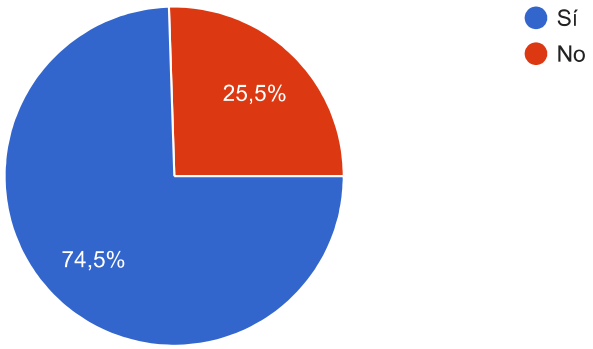


Como parte del departamento de finanzas de tu empresa recibes un correo electrónico del CEO de la misma solicitando la realización de una transferencia bancaria a un proveedor extranjero nuevo. Solicita que esta transferencia se haga con urgencia para cerrar la compra cuanto antes. La suma de dinero de esta transferencia no es una cifra relevante para la empresa.

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas

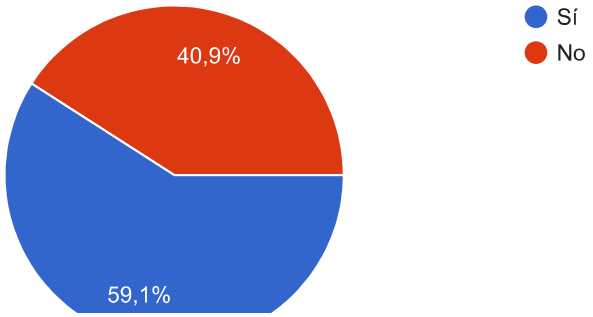


Como desarrollador en una empresa recibes un correo que contiene un archivo .zip en el que te indican que está el proyecto de una nueva aplicación. Como jefe de ese proyecto te solicitan que compruebes la calidad del software, para lo que debes descargar este archivo en tu máquina local y descomprimirlo. Normalmente utilizáis herramientas de control de versiones para los proyectos de la empresa.

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas

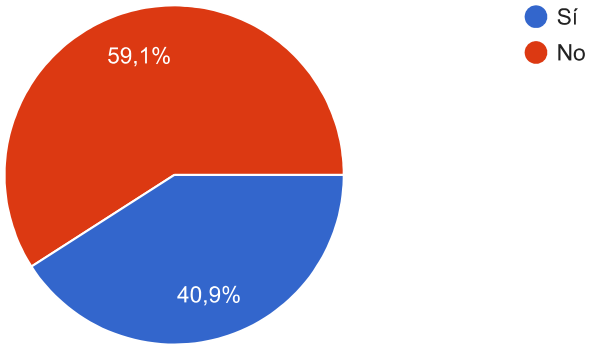


Recibes un correo de Dropbox en tu correo de empresa indicando que el almacenamiento de tu cuenta está a punto de llenarse y necesitas actualizar tu plan de suscripción. Para actualizarlo aparece un enlace en el correo que te lleva a la página oficial de Dropbox en la que ya tienes iniciada sesión.

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas

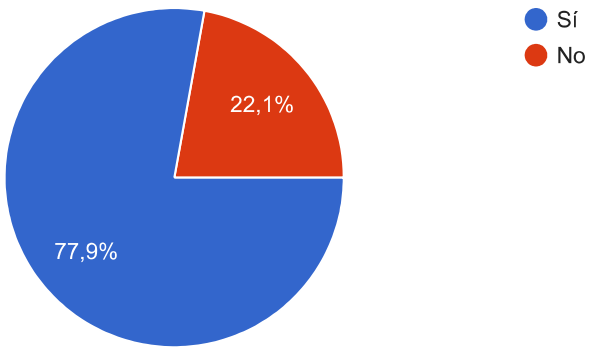


Desde la cuenta no-reply@google.support recibes un correo electrónico indicando que es posible que atacantes respaldados por un gobierno estén intentando robar tu contraseña. En el correo aparece un enlace para cambiarla. La URL de este enlace es el siguiente: www.gooogle.es/cambio-contraseña.

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas



Recibes un mensaje desde el mismo número de teléfono/conversación de la que te llegan los mensajes de los bizums, pagos que realizas, etc, de tu banco informándote de que ha habido un pago no autorizado y que para cancelarlo tienes que acceder con tus credenciales al enlace adjuntado que te dirige a una página similar a la de tu banco, pero la funcionalidad solo es esa (no te deja navegar en las otras pestañas que tiene tu banco).

Copiar

¿Consideras que este caso real es un caso de phishing?

149 respuestas