Universitat Oberta de Catalunya

uoc.edu

# Evolución e impacto del Phishing y como combatirlo.

**Autor: Carles Cano Barba**
Seguridad empresarial

**Director: Richard Rivera**

01/06/2021

**FICHA DEL TRABAJO FINAL**

| | |
|---|---|
| **Título del trabajo:** | *Evolución e impacto del Phishing y como combatirlo* |
| **Nombre del autor:** | *Carles Cano Barba* |
| **Nombre del consultor/a:** | Richard Paul Rivera Guevara |
| **Nombre del PRA:** | Víctor Garcia Font |
| **Fecha de entrega** | 06/2021 |
| **Titulación:** | *Máster Universitario en Ciberseguridad y Privacidad* |
| **Área del Trabajo Final:** | *Seguridad de Empresa* |
| **Idioma del trabajo:** | *Castellano* |
| **Palabras clave** | *Phishing, Investigación, Python.* |

**Resumen del Trabajo**

Breve investigación sobre el Phishing y su evolución, donde se pretende dar visibilidad a esta amenaza, debió al gran aumento que hubo durante la pandemia. Se pretende también aportar una pequeña herramienta con la que poder crear plantillas para poder realizar campañas de phishing a través de una herramienta de fácil uso, para ayudar a las pequeñas empresas.

Se ha conseguido obtener resultados sobre la investigación, donde se demuestra una carencia en la educación referente a ciberseguridad y donde se dan varios puntos para tener en cuenta durante el trabajo y explicados de una forma clara y con pocos tecnicismos.

**Abstract**

Brief research about Phishing and its evolution, which aims to give visibility to this threat, due to the large increase that occurred during the pandemic. It is also intended to provide a small tool for create templates and use it in phishing campaigns through an easy and free phishing tool, to help small businesses.

It has been possible to obtain results on the investigation, where it is demonstrated a lack in the education referring to cybersecurity and where several points are given for apply during the work and explained in a clear way and with few technicalities.

# Índice

## Lista de figuras

# 1. Plan de Trabajo

## 1.1 Contexto y justificación del trabajo

La situación de la pandemia actual ha hecho aumentar considerablemente la cantidad de gente que realiza teletrabajo, esto y el aumento del uso de tecnologías como las videollamadas, mails, etc. Hecho proliferar un tipo de estafa que hasta ahora no habían gozado de tanto protagonismo, este tipo de estafas es conocido como phishing ha aumentado este año mucho más que cualquier otro año, las condiciones actuales han propiciado la proliferación de esta práctica que, aunque a nivel técnico no es muy complicada de entender, sí que puede ser muy peligrosa, sobre todo en los escalones menos técnicos de las empresas. Aprovechándose de la ingeniería social para conseguir que los objetivos piquen el anzuelo y poder causar estragos en sus objetivos.

Esto queda muy bien reflejado en varios artículos que, en Internet, en concreto en septiembre IBM España revelaba que a partir de marzo del 2020 había aumentado el phishing un 6% en [1]. En enero de este año Proofpoint, empresa dedicada a la seguridad revelaba que el 60% de los CSO/CISO en España habían observado un aumento de los ataques de phishing hacia sus empresas [2], también revelaba otros datos, como por ejemplo que no siempre todos están bien preparados ante este tipo de situaciones o que muchas veces no saben exactamente quien son los principales objetivos dentro de la empresa.

Y estos datos solo han hecho que ir en aumento a lo largo del año 2020, donde gracias al informe proporcionado por Kaspersky, podemos saber cosas como esta: “España fue el principal objetivo de las campañas de correo electrónico malicioso en 2020, y su participación aumentó en 5,03 puntos, para llegar al 8,48%” [3]. Claramente España fue un claro objetivo del phishing en el último año, en el mismo informe también se menciona que las organizaciones más atacadas son las tiendas online, bancos, portales internacionales y redes sociales.

El problema del aumento de este tipo de ataques, su complejidad, diversificación y especialización, ha llevado a las empresas a buscar e implementar nuevas estrategias y formas de evitar este problema, pero algo que cambia constantemente y que evoluciona a un ritmo vertiginoso, siendo capaz de engañar cada vez a más gente, es complicado de gestionar en todos los niveles. Porque lo que parece ser un simple mail inocuo puede acabar derivando en un problema de grandes dimensiones, por lo tanto, el presente trabajo pretende centrarse en estudiar este tipo de ataques, su modus operandi, variaciones e impacto, para tener datos suficientes para poder encontrar los principales problemas a la hora de enfrentarnos al phishing.

También se estudiarán las herramientas actuales en el mercado, se evaluarán y compararán, además de preparar y desarrollar a modo de proof of concept una campaña de phishing utilizando y perfeccionando una de estas herramientas o desarrollando una nueva.

## 1.2 Objetivos del Trabajo

Los principales objetivos del trabajo son poder implementar tanto una guía para conocer y aprender sobre el phishing y cómo actuar ante él, encarada a usuarios con pocos conocimientos técnicos, así como encontrar, mejorar y actualizar una herramienta que permita mitigar y ayudar a las empresas con el phishing, manejar campañas de phishing de prueba y obtener métricas para evaluar el impacto que tendría un ataque de phishing real, o bien crear una de zero para realizar esto mismo. Para cumplir estos dos objetivos se seguirán una lista de objetivos más concretos.

Objetivos en cuanto a investigación:

- Analizar los estragos del phishing en los últimos años, a través de la recolección de datos obtenidos de diversas fuentes y obtener conclusiones al respecto.
- Evaluar el nivel de conocimiento respecto a este tipo de ataques en diferentes sectores y grupos de personas.
- A través de los datos obtenidos, generar conclusiones y puntos claves a tener en cuenta para las herramientas a utilizar.

Objetivos en desarrollo e implementación:

- Analizar el estado actual de las herramientas que hay en el mercado para la gestión del phishing y que pueden aportar al respecto, realizando una comparativa entre ellas.
- Elaborar una lista de mejoras a implementar en la herramienta escogida, para adaptarla a diferentes tipos de phishing o diferentes enfoques.
- Implementar los cambios escogidos, para mejorar la herramienta o bien implementar una herramienta de cero adaptada a los resultados de la investigación inicial.
- Realizar una prueba de concepto o PoC a modo de campaña de phishing y analizar si hemos obtenido lo que queríamos conseguir.

Objetivos en cuanto a entregables:

- Desarrollar la memoria final del trabajo, de manera que se puedan obtener unas conclusiones respecto a los datos analizados durante el trabajo.
- Una guía para usuarios no técnicos, sobre cómo actuar ante el phishing.
- Una herramienta para utilizar contra el phishing, ya sea una mejora de una actual o una nueva.

## 1.3 Enfoque y método seguido

Respecto a la metodología utilizada para este proyecto, como el proyecto cuenta con dos fases, una más encarada a la recolección de datos y análisis de estos y otra a la implementación y desarrollo de una herramienta, se dividirá el trabajo en dos fases bastante diferenciadas entre ellas.

En la parte de investigación, será una parte desarrollada más teóricamente, donde permitirá a través del estudio de los datos obtenidos y los datos recolectados el año pasado sobre phishing, obtener unas conclusiones y resultados, a partir de los cuales se decidirá como encara el apartado de implementación y desarrollo.

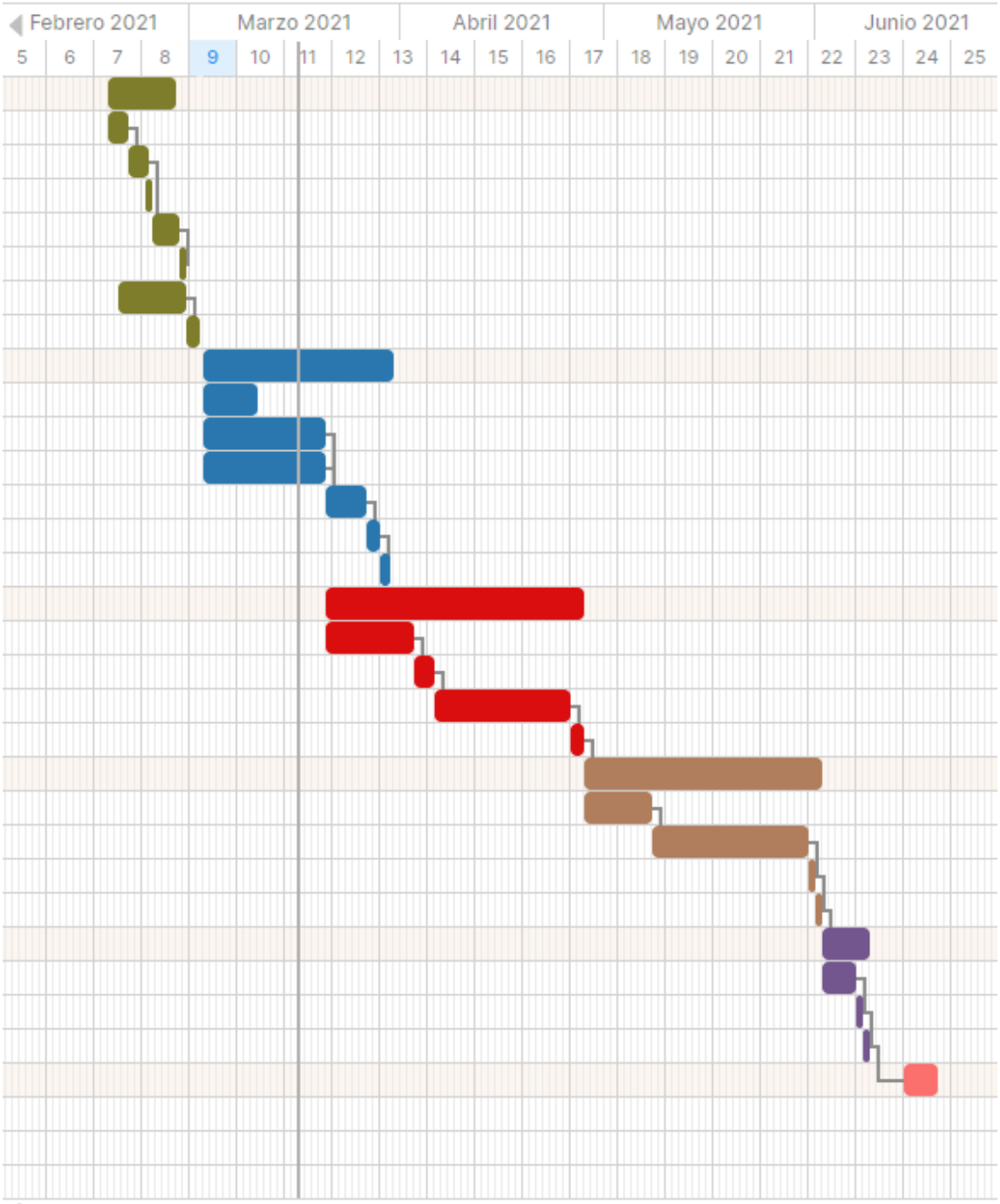
En la segunda parte, la parte más práctica se utilizarán las conclusiones obtenidas en la primera fase, para definir que implementar y como realizarlo, ya que será importante tener en cuenta los datos.

Dado que el tiempo de este proyecto es limitado, se tendrá muy en cuenta tanto los datos y conclusiones, así como los tiempos estimados que supongan ciertas decisiones, como por ejemplo el uso y mejora de una herramienta ya existente o la creación de una nueva. De manera que, una vez realizada la primera fase, se valorara o bien reajustar el proyecto y la planificación o bien seguir según lo planeado, en función de lo que se encuentre al analizar los datos, en especial la comparación de las herramientas.

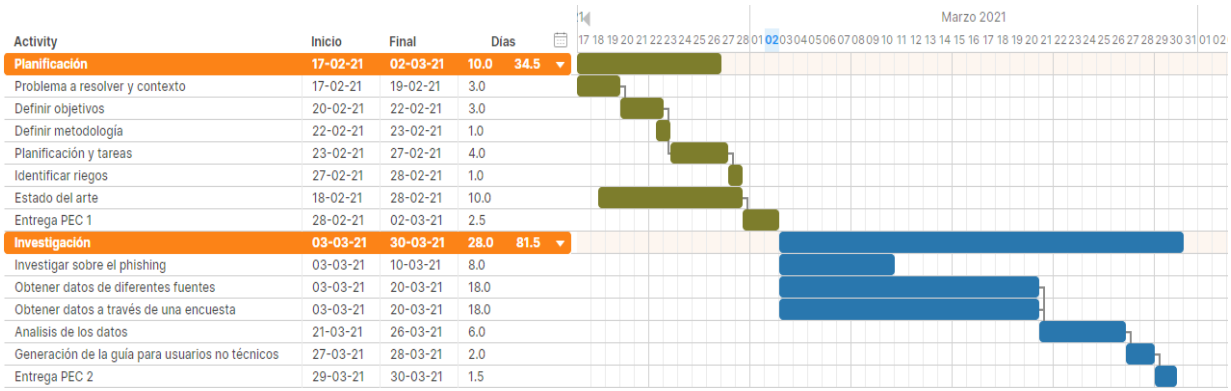
De esta forma, siguiendo estas dos fases podemos tener un mejor control del proyecto en general, para evitar no alcanzar los objetivos propuestos.

## 1.4 Tareas y planificación

| Activity | Inicio | Final | Días | |
|---|---|---|---|---|
| **Planificación** | **17-02-21** | **02-03-21** | **10.0** | **34.0** |
| Problema a resolver y contexto | 17-02-21 | 19-02-21 | 3.0 | |
| Definir objetivos | 20-02-21 | 22-02-21 | 3.0 | |
| Definir metodología | 22-02-21 | 23-02-21 | 1.0 | |
| Planificación y tareas | 23-02-21 | 27-02-21 | 4.0 | |
| Identificar riegos | 27-02-21 | 28-02-21 | 1.0 | |
| Estado del arte | 18-02-21 | 28-02-21 | 10.0 | |
| Entrega PEC 1 | 28-02-21 | 02-03-21 | 2.0 | |
| **Investigación** | **03-03-21** | **30-03-21** | **28.0** | **81.5** |
| Investigar sobre el phishing | 03-03-21 | 10-03-21 | 8.0 | |
| Obtener datos de diferentes fuentes | 03-03-21 | 20-03-21 | 18.0 | |
| Obtener datos a través de una encuesta | 03-03-21 | 20-03-21 | 18.0 | |
| Analisis de los datos | 21-03-21 | 26-03-21 | 6.0 | |
| Generación de la guía para usuarios no técnicos | 27-03-21 | 28-03-21 | 2.0 | |
| Entrega PEC 2 | 29-03-21 | 30-03-21 | 1.5 | |
| **Implementación y desarrollo** | **21-03-21** | **27-04-21** | **38.0** | **76.0** |
| Análisis de las herramientas actuales | 21-03-21 | 02-04-21 | 13.0 | |
| Decisión sobre la herramienta a implementar | 03-04-21 | 05-04-21 | 3.0 | |
| Implementación de mejoras o de la herramienta | 06-04-21 | 25-04-21 | 20.0 | |
| Entrega PEC 3 | 26-04-21 | 27-04-21 | 2.0 | |
| **Memoria Final** | **28-04-21** | **01-06-21** | **35.0** | **70.0** |
| Realización de la PoC | 28-04-21 | 07-05-21 | 10.0 | |
| Redacción de la memoria | 08-05-21 | 30-05-21 | 23.0 | |
| Revisión de la memoria | 31-05-21 | 31-05-21 | 1.0 | |
| Entrega PEC 4 | 01-06-21 | 01-06-21 | 1.0 | |
| **Presentación en vídeo** | **02-06-21** | **08-06-21** | **7.0** | **14.0** |
| Realización del vídeo | 02-06-21 | 06-06-21 | 5.0 | |
| Revisión del vídeo | 07-06-21 | 07-06-21 | 1.0 | |
| Entrega Vídeo | 08-06-21 | 08-06-21 | 1.0 | |
| **Defensa del TFM** | **14-06-21** | **18-06-21** | **5.0** | **5.0** |

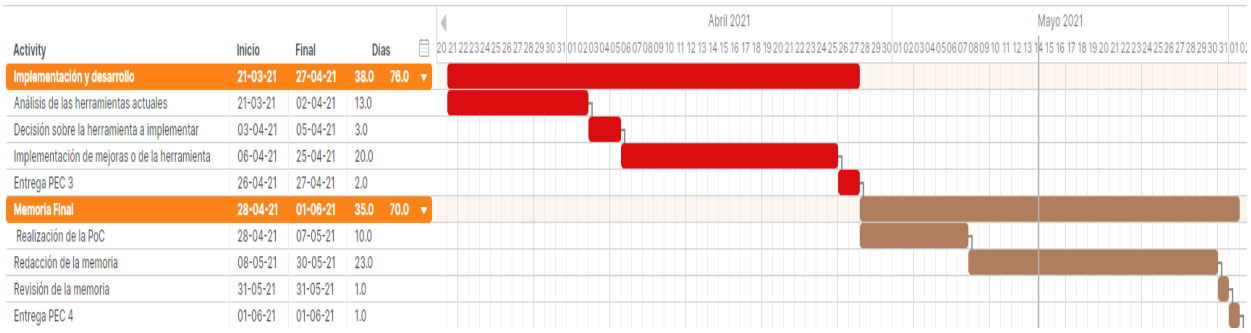

Febrero 2021
Marzo 2021
Abril 2021
Mayo 2021
Junio 2021
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

- Planificación e Investigación



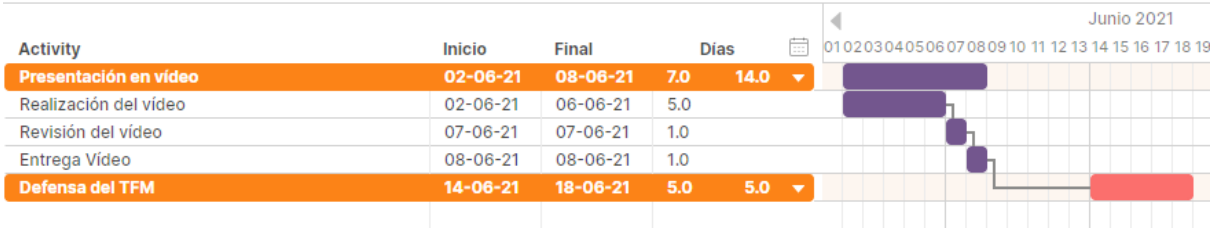
| Activity | Inicio | Final | Días | |
|---|---|---|---|---|
| **Planificación** | **17-02-21** | **02-03-21** | **10.0** | **34.5** |
| Problema a resolver y contexto | 17-02-21 | 19-02-21 | 3.0 | |
| Definir objetivos | 20-02-21 | 22-02-21 | 3.0 | |
| Definir metodología | 22-02-21 | 23-02-21 | 1.0 | |
| Planificación y tareas | 23-02-21 | 27-02-21 | 4.0 | |
| Identificar riegos | 27-02-21 | 28-02-21 | 1.0 | |
| Estado del arte | 18-02-21 | 28-02-21 | 10.0 | |
| Entrega PEC 1 | 28-02-21 | 02-03-21 | 2.5 | |
| **Investigación** | **03-03-21** | **30-03-21** | **28.0** | **81.5** |
| Investigar sobre el phishing | 03-03-21 | 10-03-21 | 8.0 | |
| Obtener datos de diferentes fuentes | 03-03-21 | 20-03-21 | 18.0 | |
| Obtener datos a través de una encuesta | 03-03-21 | 20-03-21 | 18.0 | |
| Analisis de los datos | 21-03-21 | 26-03-21 | 6.0 | |
| Generación de la guía para usuarios no técnicos | 27-03-21 | 28-03-21 | 2.0 | |
| Entrega PEC 2 | 29-03-21 | 30-03-21 | 1.5 | |

- Implementación y Memoria Final



| Activity | Inicio | Final | Días | |
|---|---|---|---|---|
| **Implementación y desarrollo** | **21-03-21** | **27-04-21** | **38.0** | **76.0** |
| Análisis de las herramientas actuales | 21-03-21 | 02-04-21 | 13.0 | |
| Decisión sobre la herramienta a implementar | 03-04-21 | 05-04-21 | 3.0 | |
| Implementación de mejoras o de la herramienta | 06-04-21 | 25-04-21 | 20.0 | |
| Entrega PEC 3 | 26-04-21 | 27-04-21 | 2.0 | |
| **Memoria Final** | **28-04-21** | **01-06-21** | **35.0** | **70.0** |
| Realización de la PoC | 28-04-21 | 07-05-21 | 10.0 | |
| Redacción de la memoria | 08-05-21 | 30-05-21 | 23.0 | |
| Revisión de la memoria | 31-05-21 | 31-05-21 | 1.0 | |
| Entrega PEC 4 | 01-06-21 | 01-06-21 | 1.0 | |

- Presentación en vídeo y Defensa



| Activity | Inicio | Final | Días | |
|---|---|---|---|---|
| **Presentación en vídeo** | **02-06-21** | **08-06-21** | **7.0** | **14.0** |
| Realización del vídeo | 02-06-21 | 06-06-21 | 5.0 | |
| Revisión del vídeo | 07-06-21 | 07-06-21 | 1.0 | |
| Entrega Vídeo | 08-06-21 | 08-06-21 | 1.0 | |
| **Defensa del TFM** | **14-06-21** | **18-06-21** | **5.0** | **5.0** |

## 1.5 Riesgos Preliminares

Se han identificado los principales riesgos que pueden afectar de manera negativa a la planificación del trabajo. Pudiendo perjudicar al resultado final o incluso haciendo peligrar cumplir los objetivos marcados inicialmente, también se propone una mitigación para cada uno de ellos.

- **Riesgo 1: Alcance excesivo**
  El alcance inicial del proyecto es demasiado elevado para los tiempos estimados o los imprevistos son excesivos.
  Impacto en el proyecto: Alto
  Probabilidad: Media
  Mitigación: Simplificación de la parte de desarrollo, simplificar la prueba de concepto o eliminar tareas que sean menos importantes.

- **Riesgo 2: Falta de datos**
  Problemas con la obtención de los datos respecto al phishing.
  Impacto en el proyecto: Alto
  Probabilidad: Baja
  Mitigación: Uso de los pocos datos que podamos obtener.

- **Riesgo 3: Complejidad**
  La implementación de las herramientas se vuelve complicada o requiere de más estudio.
  Impacto en el proyecto: Medio
  Probabilidad: Baja
  Mitigación: Buscar soporte externo para las tareas que requieran una complejidad más elevada o buscar alternativas más simples.

- **Riesgo 4: Problemas para realizar la PoC**
  Podría darse el caso de que no pudiese realizarse la PoC en un entorno real, que sería el mejor entorno.
  Impacto en el proyecto: Bajo
  Probabilidad: Media
  Mitigación: Realizar una PoC en un entorno controlado o modificarla para que sea lo más inocua posible.

## 1.6 Estado del arte

Aunque actualmente hay estudios sobre ciberamenazas [4] y el impacto de estas, no hay tantos centrándose en el phishing a pesar de ser una de las amenazas más comunes y fáciles de evitar.

Existen diversos estudios, pero ninguno con datos actualizados, otros muchos son de empresas grandes del sector que o bien no enseñan todo o bien cuesta encontrarlos, las guías sobre phishing acaban siendo más de lo mismo, se basan demasiado en conceptos técnicos o entran demasiado en detalle.

Otras organizaciones como INCIBE [5], si cuentan con herramientas útiles y hasta kits de "concienciación", pero la mayoría de la gente no es consciente de que existen este tipo de organizaciones, ni mucho menos que ofrecen este tipo de guías. Sí que es cierto que tienen mucha información, pero por ejemplo mucha gente no sabe que es un "link" o que es "*web spoofing*" son términos muy técnicos, por lo que mi guía pretende ser mucho más visual y simple, para poder abarcar al máximo de público posible, puesto que actualmente no existen este tipo de estudios que expone claramente y para todo el mundo que es el phishing y cómo puede cualquier persona protegerse de ello.

En lo que respecta a herramientas, existen varias empresas en el sector privado que ofrecen sus servicios para que otras empresas cuenten con entrenamientos específicos de phishing mediante campañas de pruebas y concienciación. En cuanto a lo que se refiere a herramientas *open source* y con capacidad de personalización con entornos específicos o situaciones concretas, esto no es tan fácil de encontrar.

Algunas herramientas cuentan con una buena comunidad detrás, pero podrían mejorar exponencialmente actualizando la herramienta o añadiendo nuevas funcionalidades a esta, es el caso de Gophish, una buena herramienta de la que podría sacarse mucho más utilizando los datos y las conclusiones correctas. También contamos con otras, que les falta actualizarse, porque, aunque siguen manteniéndose, no son del todo sencillas de entender, ni mucho menos sacar datos, como por ejemplo King Phisher.

En las que respecta a las privadas, algunas cuentan con herramientas "demo" o con uso limitado de sus características, pero que parece que en muchos casos no siempre es suficiente.

Este apartado se desarrollará en más profundidad y con muchos más datos tras realizar las investigaciones necesarias.

# 2. Breve historia del Phishing

## 2.1 Los comienzos del Phishing

El phishing como tal, no es algo nuevo, no ha aparecido de la nada. Es algo que está casi desde los inicios de Internet y que ha ido evolucionando con el tiempo y a su vez especializándose y mejorando.

El primer uso del término phishing data de enero de 1996 en el grupo de noticias de hackers alt.2600 y fue usado para denominar a quienes intentaban "pescar" cuentas de miembros de AOL. Este phishing tenía como objetivo principal la obtención de los datos y credenciales de las víctimas potenciales, haciéndose pasar por empleados de AOL.

A partir de ese momento y con la salida de los antiguos gigantes del correo en Internet como Yahoo y Hotmail, empezó a aparecer lo que comúnmente llamamos phishing, pero de una forma masiva. Este phishing era bastante diferente a lo que hoy conocemos, eran mails mucho menos trabajados, enfocados a llegar a un gran número de gente y con poca personalización, lo que los hacía fácilmente detectables y que muchas veces no salían ni de la carpeta de spam.

Con la entrada en escena de los programas de mensajería instantánea como MSN Messenger, empezó a diversificarse este tipo de prácticas y a evolucionar gracias a la ingeniería social, llegando al punto en donde nos encontramos ahora.

## 2.2 Impacto y expansión debido al COVID

Ha habido un factor clave este último año que ha hecho dispararse el número de casos de phishing y el impacto de estos. La aparición de la pandemia, debido al COVID, ha propiciado el aumento del teletrabajo y del uso masivo de las redes sociales [6], [4]. Este hecho por si solo parece no tener mucha relación, puesto que el phishing hace años que existe, pero la evolución constante del phishing hizo que este se valiera de la personalización y del uso de la pandemia como gancho, para que durante los primeros meses se multiplicaran los casos de phishing en España.

Este efecto siguió avanzando y aumentando, expandiéndose no solo a mails relacionados con la pandemia, si no también valiéndose del paso a internet de gran cantidad de servicios, como, por ejemplo: bancos online, mensajería y paquetería, compras online y gestiones con las administraciones públicas como hacienda.

Esto ha hecho que pasemos del simple mail suplantando a una compañía concreta, a un amplio abanico de ataques relacionados con el phishing.

## 2.3 Enfoque del Phishing

La evolución del phishing ha hecho que actualmente este cuente con diferentes tipos, en función de cómo se interactuar con la víctima o el objetivo de este phishing, para poder ver estas evoluciones de cómo realizar phishing a día de hoy, describiremos brevemente algunos de los diferentes métodos, sus nombres y cómo funcionan.

**Phishing tradicional:** Este phishing es el que la mayoría de gente conoce como tal, es el típico correo, nada especializado y que suele intentar suplantar a una empresa o gran compañía que inspire confianza. Se suele ver fácilmente que no es un correo legítimo, suele contener faltas o está mal estructurado, además suele exigir algo con urgencia o llamando la atención por algo en concreto, para acabar obteniendo las credenciales de la víctima. [7]

**Smishing:** Uno de los tipos que ha aumentado muchísimo últimamente, este a diferencia del primero suele llegarnos al móvil a partir de un SMS. Este SMS contiene un enlace o número de teléfono a donde llamar, que es donde está la estafa realmente. Ha aumentado la proliferación de este tipo en concreto, porque están aprovechando un factor y negocio que también ha aumentado, este factor clave es el comercio electrónico, donde esos SMS que recibimos intentan suplantar empresas de mensajería y paquetería que pretenden traerte una de tus compras online a casa. [7]

**Vishing:** este tipo de phishing modifica un poco el método, puesto que en este caso se realiza la estafa mediante voz, ya sea por una llamada de teléfono o por Skype, Teams o similares. Es bastante habitual en el vishing hacerse pasar por una compañía, como por ejemplo un banco o una tecnológica como Microsoft. [7]

**Spear phishing:** este tipo de phishing es muy parecido al primer caso descrito, pero la diferencia reside en el objetivo. El phishing tradicional no suele tener un objetivo concreto, es un envío masivo de un correo igual para todos los objetivos con alguna mínima personalización. En cambio, el spear phishing está centrado en el objetivo, de forma que se decide y concreta un objetivo concreto como puede ser una persona concreta o un grupo de personas con características y de entorno similares. Esto hace que los correos sean mucho más especializados y personalizados, de forma que cuesta mucho más saber si es legítimo lo que estamos recibiendo o no. [8]

**Whaling:** Es similar al spear phishing puesto que tiene un objetivo concreto, pero en este caso el objetivo de este tipo de phishing son altos cargos de empresas, representantes de grandes tecnológicas o directivos. Pero el objetivo principal no son estos altos cargos, es decir, estos altos cargos no recibirán el mail, si no que serán utilizarlos como gancho para que la víctima final se crea que el mail es legítimo. De forma que haciéndose pasar por su jefe o un alto directivo de la empresa, los empleados recibirán un mail que inspire más confianza y que tenga más posibilidad de ser abierto y de caer en la trampa. [9]

# 3. Fases del Phishing

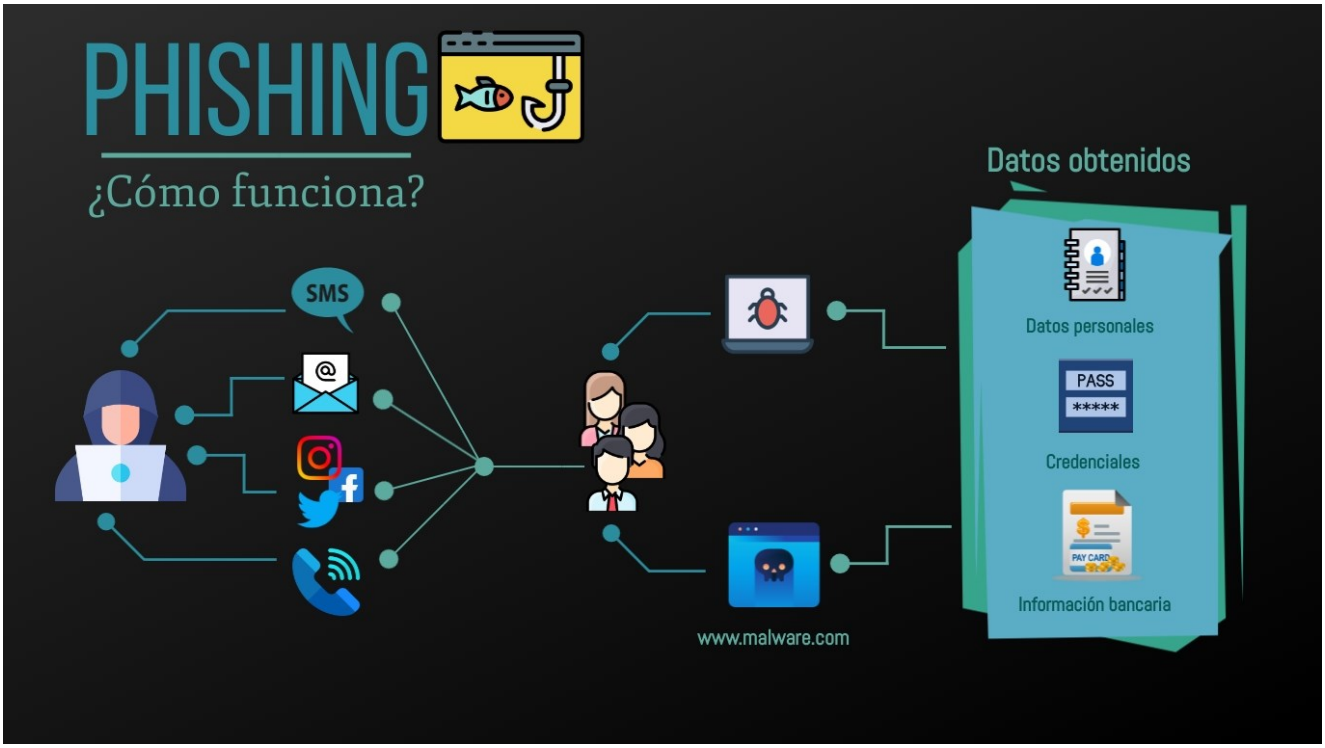



*Ilustración 1 Esquema del funcionamiento del phishing*

En la imagen anterior tenemos un esquema del funcionamiento del phishing, que podemos dividir en varias fases, aunque no siempre hay porque seguir un orden, estas fases se describen a continuación.

## 3.1 Selección del método

El atacante debe decidir el tipo o método de transmisión, es decir, como hará llegar a la víctima el phishing.

Si se utiliza un SMS, un correo, un mensaje por redes sociales o una llamada de dándole instrucciones. Esto dependerá también de los recursos del atacante para obtener los datos, no es lo mismo conseguir un correo que un número de teléfono, incluso puede ser que utilice algún otro malware o una base de datos vulnerada para poder obtener este tipo de datos de la víctima. Una vez decidido se procederá con alguna de las siguientes fases.

## 3.2 Elección del objetivo

La elección del objetivo es una parte importante del phishing, por no decir que podría ser una de las más importantes dependiendo del caso. Como se puede entender simplemente, esta fase puede ir incluso antes de la elección del método, un ejemplo claro de esto es el *spear phishing*, donde desde un primer momento se tiene un objetivo concreto.

El proceso de elección no es algo trivial, puesto que en muchos casos requiere del estudio del objetivo, por ejemplo, si se pretende realizar un phishing a una empresa es muy habitual estudiar a donde enviar este phishing. Ya que, es mucho más probable que el personal técnico y de IT de la empresa, puedan detectar la estafa antes que alguien de administración sin este tipo de conocimientos.

En cambio, si se realiza un phishing clásico, esta selección de objetivos puedes ser mucho menos elaborada. Por ejemplo, se cogerá una base de datos de móviles filtrados y se realizara sobre ella una campaña de phishing con SMS genéricos para todos, como es el caso de los últimos phishing sustituyendo empresas de paquetería.

## 3.3 Ingeniería social

Una parte poco conocida del phishing, pero importante en el proceso para desarrollar un ataque exitoso es la ingeniería social.

Si buscamos ingeniería social en internet encontraremos muchas definiciones, como por ejemplo las siguientes:

- **Wikipedia** [10]**:** La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.
- **Web de Avast** [11]**:** La ingeniería social consiste en engañar a la gente para que cedan su información personal como contraseñas o datos bancarios o para que permitan el acceso a un equipo con el fin de instalar software malicioso de forma inadvertida.
- **Web de Kaspersky** [12]**:** La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Como podemos ver en este pequeño recopilatorio, podemos resumir que la ingeniería social es el engaño y manipulación de la víctima para obtener algo a cambio.

El papel que juega la ingeniería social [13] en este proceso es simple, estudiar y elaborar la forma de que mediante SMS, mail, mensaje o voz se consiga engañara a la víctima para que realice un procedimiento concreto. Ya sea entrar en una web o descargar algún archivo, para poder finalmente obtener datos, conseguir acceso a su máquina u obtener credenciales.

Para que este proceso de resultado es mucho mejor tratar de obtener toda la información posible sobre el objetivo. De forma que, si por ejemplo tratamos con una empresa de seguros, enviar un mail sobre un siniestro podría ser una buena idea, que podría mejorarse si se consigue los datos que se suelen intercambiar entre un cliente y la empresa. También es una práctica muy utilizada tratar temas de actualidad, como ejemplo más claro temas como “nuevas políticas de protección individual ante el COVID” o “Nuevos procesos de seguridad para evitar ciberataques debido al caso SEPE”, podrían ser claves para conseguir que una víctima abra un mail y descargue un archivo malicioso.

## 3.4 Vector de ataque

Esta fase podríamos llamar “vector de ataque”, pues se trata de la amenaza o la forma en que realizaremos el ataque propiamente dicho, es la parte más técnica del proceso puesto que hay que tener en cuenta varios factores. Para empezar, se debe escoger el objetivo del ataque, esto encuadra diferentes opciones [14], [15], [16]:

- Realizar el máximo daño posible, como ejecutar malware para eliminar y bloquear el sistema.
- Obtener un beneficio, como por ejemplo ejecutar un ransomware y pedir un rescate de la máquina.
- Obtener unos datos concretos, como credenciales o datos de usuarios.
- Obtener acceso a información confidencial o de acceso restringido y limitado.

Se debe decidir cómo se realizar el ataque, si se utilizara un archivo con el que comprometer el dispositivo de la víctima o si se utilizará una web externa para obtener datos de la víctima, como credenciales o parecidos. Estos dos métodos son los más habituales y comunes en los ataques, aunque existen otros como uno que se ha estado llevado a cabo últimamente a través de whatsapp, que consiste en pedir el código de verificación de whatsapp a la víctima para poder suplantarlo en esta plataforma.

Cada método tiene sus pros y sus contras, si se utiliza un archivo hay bastantes factores para tener en cuenta [17], [18], [19]:

- Tipo de archivo que se utilizara: PDF, zip, Word, etc.
- Detección automática de mails de phishing.
- Detección del archivo descargado por el antivirus
- ¿Sera necesaria interacción con el archivo por parte de la víctima?

Aunque es más complicado de conseguir que funcione, su función suele tener mucho más impacto en el objetivo, pudiendo conseguir muchas más cosas que utilizando una web. Por otra parte, si se utiliza una web hay que tener en cuenta estos otros factores:

- ¿Qué datos se quieren obtener? Bancarios, credenciales de mail, etc.
- ¿Qué web se utilizará? Una clon de la original, una creada por el atacante, etc.
- El proceso de petición de los datos: se pedirá un login directamente, un proceso más elaborado, algún tipo de error de login, etc.

Aunque es más fácil de implementar que el anterior y suele ser más fácil de que el ataque sea exitoso, está limitado por lo que es, puesto que es más complicado de que tenga la capacidad de obtención de datos o de dañar al objetivo que tiene el método del archivo.

## 3.5 Obtención de resultados

Por último, simplemente quedaría por pate del atacante recoger los datos obtenidos o cumplir con los objetivos del ataque. Estos, como se ha comentado

ya, pueden ir desde a partir de los datos bancarios de la víctima robarle dinero, utilizar sus credenciales para acceder a información privilegiada o incluso realizar gestiones con sus datos personales, como contratar servicios a su nombre. Por último, también se podría ganar acceso a su máquina e instalar programas maliciosos para realizar chantaje, como un ransomware o algún software de recopilación de información.

# 4. Análisis de los resultados de la encuesta

Para poder tener una pequeña visión del conocimiento a pie de calle, sobre lo explicado anteriormente sobre phishing, se ha realizado una encuesta a un total de 340 personas de diferentes entornos y generaciones.

En este apartado se pretende analizar los resultados obtenidos, para poder sacar conclusiones sobre el conocimiento general respecto al phishing en la sociedad actual. En la encuesta hay preguntas generales y una bifurcación en función de si conoces el término phishing o no, también hay que destacar que, para evitar hacer una distinción en cuanto a edad, se ha determinado unos rangos correspondientes a generaciones. Estos rangos son la generación del baby boom, generación X, milenials, etc. Esto se ha realizado de esta manera, porque es un indicativo mejor y que se hace más fácil de encajar con los diferentes avances tecnológicos, también se les ha pedido a los encuestados el rango de estudios.

De las 340 personas encuestadas, más de la mitad, un 55,6% desconocían por completo el término “Phishing”, a pesar de la época en la que vivimos donde es constante ver noticias al respecto en todos los medios.

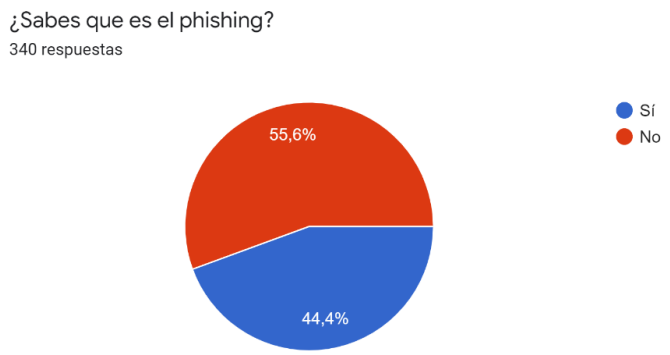



*Ilustración 2 Resultados de la pregunta “¿Sabes que es el phishing?” de la encuesta.*

Para ayudar a la gente a comprender sobre que se estaba hablando en la encuesta, se proporcionó esta pequeña descripción:

“*El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información*

*confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima."*

De las 189 personas que respondieron que no a si sabían que era el phishing, al menos 48 personas, a pesar de leer la definición, seguirían sin saber reconocer una de estas estafas. Se podría sacar conclusiones erróneas sobre estas 48 personas, por ejemplo, dos conclusiones rápidas que se podrían hacer sin conocer los datos podrían ser que son gente "mayor" y que por lo tanto no controla sobre temas de tecnología o, por otra parte, que son gente con pocos estudios.

Pero estas conclusiones, están lejos de la realidad puesto que, de esas 48 personas, al menos un 33,33%, es decir, 16 personas de estas 48 que niega saber que es el phishing a pesar de leer su definición, son personas jóvenes nacidos a partir de 1980, pertenecientes a la generación de los milenials o a la generación Y.

Pero estos datos no son una mera casualidad, puesto que si nos remitimos a la pregunta anterior: "¿Sabes que es el phishing?". De un total de 340 personas que respondieron, el 28,82% de los encuestados, unas 98 personas desconocían que era el phishing a pesar de pertenecer a las generaciones de los milenials y la generación Y, es decir, tenemos que casi 1/3 de los encuestados desconocen que es el phishing, a pesar de ser jóvenes y haber nacido en épocas donde han podido aprender de la mano de la tecnología.

Por otro lado, en lo que respecta a estudios, tenemos que al menos 9 personas de las 48 que respondieron que no conocían que era el phishing ni lo reconocerían a pesar de leer la descripción. Tienen estudios universitarios, otros 9 tienen algún tipo de formación profesional y 5 tiene Bachillerato o similares.

Por lo que un 47,9% de las 48 personas, es decir 23 de ellas, cuentan con estudios postobligatorios, lo que deja claro que no es un tema de estudios.

Como en el caso anterior queda confirmada esta tendencia, puesto que si lo traspasamos a la pregunta: "¿Sabes que es el phishing?". Hay un total de 144 personas con estudios postobligatorios, es decir un 42,35 % de las 340 personas encuestadas que desconocen que es el phishing.

En lo que respecta a las personas que sí que conocían que es el phishing, también se pueden conseguir conclusiones interesantes. Por ejemplo, más de la mitad de los 151 encuestados que respondieron que conocían que es el phishing, conocen a alguien que lo ha sufrido.


*Ilustración 3 Resultados de la pregunta "¿Conoces a alguien que haya tenido problemas por el phishing?" de la encuesta*

Además de este dato bastante revelador, también vemos que casi la mitad no sabría cómo actuar si fueran ellos mismos los afectados por este tipo de estafas.


*Ilustración 4 Resultados de la pregunta "¿Sabes cómo hay que actuar si algún día te llega a suceder?" de la encuesta*

Estos últimos datos, reflejan un problema clave, puesto que la mitad de las personas que tienen conocimiento sobre phishing no saben cómo actuar si les llegara a suceder, esto refleja que a pesar de saber y conocer sobre la amenaza carecen de los conocimientos para saber cómo proceder si se ven afectados.

Estos conocimientos podrían llegar a ser clave para evitar daños mayores, puesto que el tiempo de reacción ante el phishing es clave, para su mitigación y su procesamiento para aplicar procesos de respuesta a incidentes cuanto antes.

Por otro lado, también se les pregunto a cerca de los diferentes tipos de phishing, para saber o para tener, una pequeña visión de que sabían realmente.

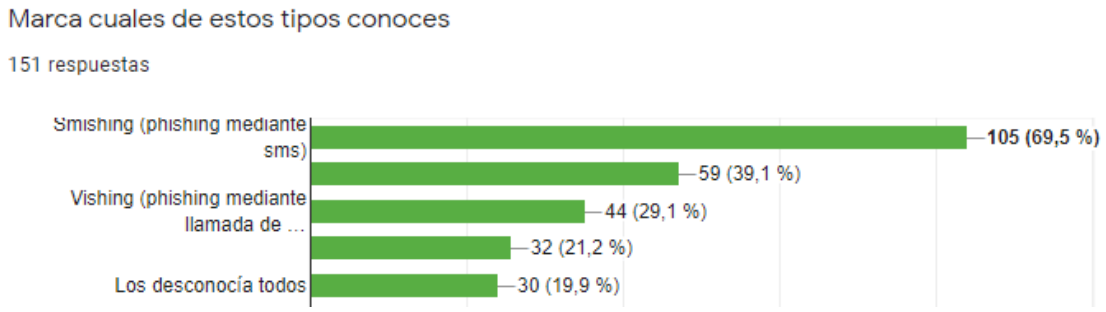



*Ilustración 5 Resultados respecto a los tipos de phishing planteados en la encuesta.*

Claramente los datos reflejan que el más conocido por todos es el Smishing con un 69,5%, seguramente debido a la cantidad de noticias y avisos que han salido últimamente sobre el tema. Spear phishing, Vishing y Whaling comparten datos similares en cuanto a conocimiento de ellos, seguramente porque son menos típicos. Por últimos tenemos un casi 20% de los encuestados que desconocen estos tipos, seguramente debido a que lo vean todo como phishing o por simple desconocimiento de los términos.

Otro dato interesante es que casi un 20% de ellos desconocía que existen diferentes tipos, algo que no es de extrañar debido al tecnicismo de los nombres y que es complicado el conocimiento de todos ellos.

También se planteó la pregunta de "¿Te dan algún curso o recomendación en tu Escuela/Instituto/Trabajo, para prevenir este tipo de estafas en Internet?"

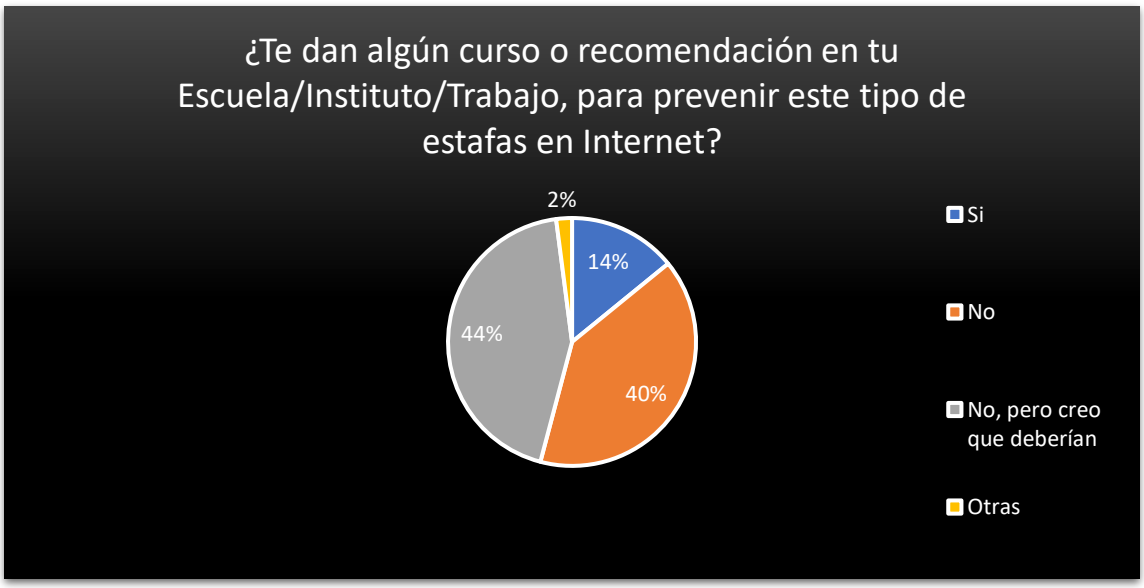



*Ilustración 6 Resultados respecto a la pregunta "¿Te dan algún curso o recomendación en tu Escuela/Instituto/Trabajo, para prevenir este tipo de estafas en Internet?"*

Como se puede ver en los datos anteriores, solo un 14% (48 personas) de todos los encuestados reciben formación específica para poder estar prevenidos sobre el phishing. Es un dato muy bajo, sabiendo el aumento en los últimos años de este tipo de estafas, que un 88% (285 personas) de los encuestados no reciban ninguna formación ni en la escuela, da una clara evidencia de la falta de formación en ciberseguridad, además un 40%, la mitad de los que no reciben formación, si creen que deberían recibir tal formación.

Por último, como dato final en este análisis se les pregunto a los encuestados lo siguiente: "¿Crees que cada vez es más complicado distinguir estafas en Internet?"

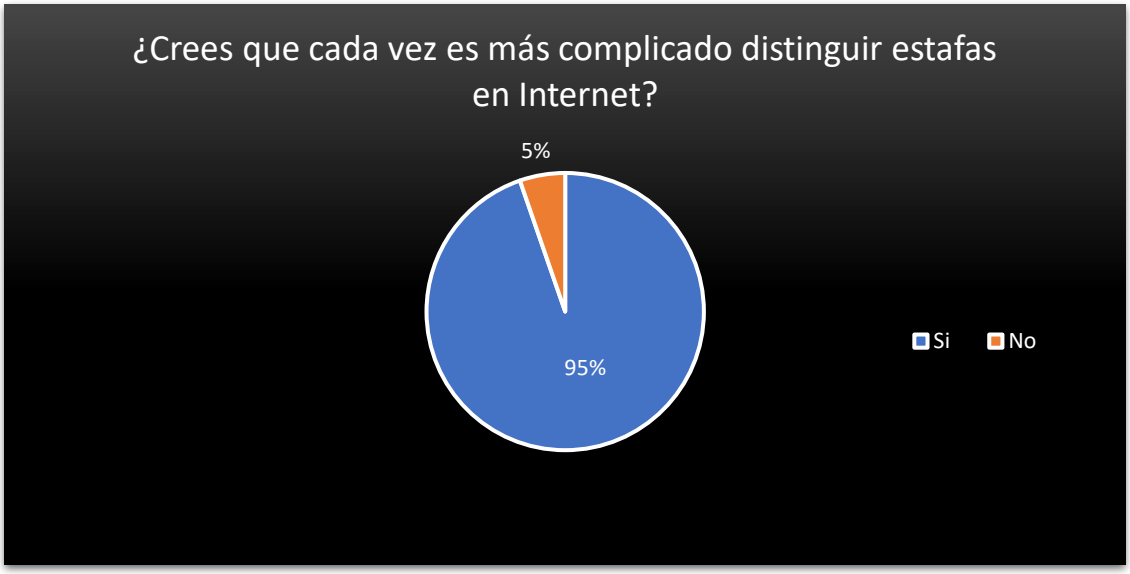



*Ilustración 7 Resultados a la pregunta ¿Crees que cada vez es más complicado distinguir estafas en Internet?*

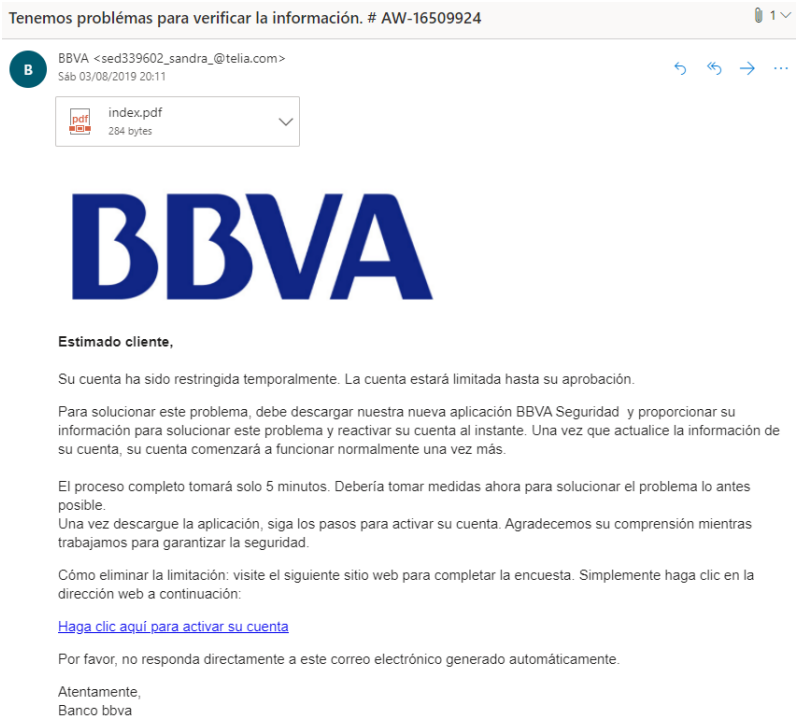
Claramente existe una preocupación sobre la capacidad para poder detectar estafas en Internet, el phishing es un buen ejemplo de ello. Está claro que, si el 95% de las personas encuestadas creen que cada vez es más complicado distinguir este tipo de estafas, es porque existe una preocupación por este tema y es algo que seguramente ira aumentando.

# 5. Análisis de smshing y phishing vía mail

Para saber cómo debe ser un mail de phishing o un sms se ha realizado una pequeña recogida de muestras para analizar algunos de los métodos más utilizados y con los que los usuarios tienen que lidiar a diario.

Realmente son muy parecidos, lo único que cambia entre el SMS y el mail es el medio, pero las técnicas utilizadas son las mismas.

Una de las tácticas más utilizadas es utilizar a una compañía como puede ser un banco o una empresa de *delivery*. La clave de estos mails es introducir términos que llamen la atención del objetivo, como en este caso:


Tenemos problémas para verificar la información. # AW-16509924

BBVA <sed339602_sandra_@telia.com>
Sáb 03/08/2019 20:11

index.pdf
284 bytes

BBVA

**Estimado cliente,**

Su cuenta ha sido restringida temporalmente. La cuenta estará limitada hasta su aprobación.

Para solucionar este problema, debe descargar nuestra nueva aplicación BBVA Seguridad y proporcionar su información para solucionar este problema y reactivar su cuenta al instante. Una vez que actualice la información de su cuenta, su cuenta comenzará a funcionar normalmente una vez más.

El proceso completo tomará solo 5 minutos. Debería tomar medidas ahora para solucionar el problema lo antes posible.
Una vez descargue la aplicación, siga los pasos para activar su cuenta. Agradecemos su comprensión mientras trabajamos para garantizar la seguridad.

Cómo eliminar la limitación: visite el siguiente sitio web para completar la encuesta. Simplemente haga clic en la dirección web a continuación:

Haga clic aquí para activar su cuenta

Por favor, no responda directamente a este correo electrónico generado automáticamente.

Atentamente,
Banco bbva

*Ilustración 8 Captura de un mail de phishing suplantando el BBVA*

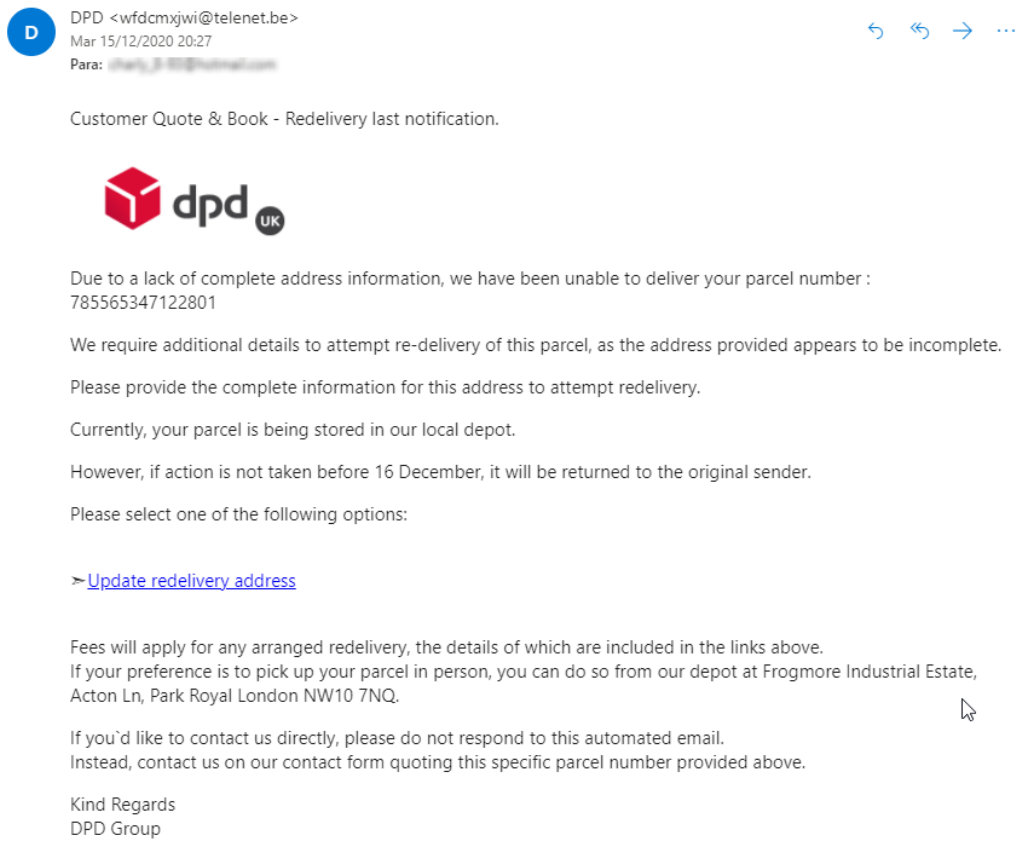
Como se puede comprobar, en este caso se pide verificar una información, se dan instrucciones y se genera cierta sensación de urgencia, con frases como “para solucionar el problema cuanto antes posible” o “su cuenta ha sido restringida temporalmente”.

También vemos otros datos llamativos, se utiliza un logo grande dando sensación de que es el mismo banco quién envía el mail. Otro dato llamativo que es muy habitual es esconder o enmascarar el link, para evitar ver a la página donde se redirige.

Como puntos claves que nos avisan de que es phishing, tendríamos dos muy llamativos, el primero y más claro es el mail de origen, que claramente puede

verse que no parece ser algo del BBVA y la otra es algo bastante común en este tipo de mails, que son las faltas de ortografías en este caso se pueden encontrar en el mismo asunto: “Tenemos **problémas** para verificar la información”

A continuación, tenemos otro más actual donde hay algún otro aspecto a tener en cuenta:


DPD <wfdcmxjwi@telenet.be>
Mar 15/12/2020 20:27
Para:

Customer Quote & Book - Redelivery last notification.

dpd UK

Due to a lack of complete address information, we have been unable to deliver your parcel number : 785565347122801

We require additional details to attempt re-delivery of this parcel, as the address provided appears to be incomplete.

Please provide the complete information for this address to attempt redelivery.

Currently, your parcel is being stored in our local depot.

However, if action is not taken before 16 December, it will be returned to the original sender.

Please select one of the following options:

➢Update redelivery address

Fees will apply for any arranged redelivery, the details of which are included in the links above.
If your preference is to pick up your parcel in person, you can do so from our depot at Frogmore Industrial Estate, Acton Ln, Park Royal London NW10 7NQ.

If you`d like to contact us directly, please do not respond to this automated email.
Instead, contact us on our contact form quoting this specific parcel number provided above.

Kind Regards
DPD Group

*Ilustración 9 Captura de mail suplantando dpd*

En este caso, tenemos otro mail intentando suplantar a una empresa de paquetería, tenemos elementos en común con el anterior, el link está oculto, logo de la empresa original, pero también se pueden ver cosas extrañas que igual un usuario normal no sabría identificar pero que alguien técnico sí. Parece que el mail habla en todo momento de UK pero el dominio del mail de origen es .be que corresponde a Bélgica, por otro lado parece extraño que una empresa profesional utilice un mail con nombre “wfdcmxjwi” para gestionar sus envíos.

Por otro lado, hay que ser un poco conscientes y en este caso si no se ha realizado ningún pedido que viene de UK o que utiliza esta compañía, debería de alguna forma alertar al usuario de que esto puede ser un fraude.

En este caso, se puede incluso examinar el hipervínculo para poder analizar a donde dirige. Para ello se puede utilizar multitud de páginas, pero una de las más utilizadas es Virustotal.

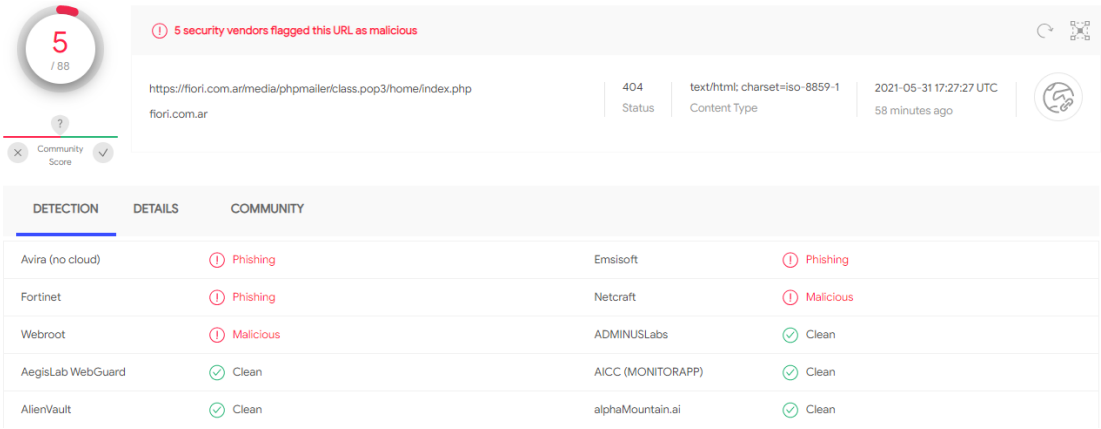



*Ilustración 10 Virus total examina la URL del link del mail.*

En la imagen anterior, se puede ver el análisis que realiza virustotal sobre la URL

que contenía el mail. Se puede ver que ya hace saltar varias alarmas que dice que esta URL es Phishing o un sitio malicioso.

Además, también hay otro factor llamativo, si se analiza la URL veremos que el dominio es **https://fiori.com.ar/** **,** es decir, es un dominio de un sitio argentino lo que no encaja de ninguna forma con el mail inicial de la empresa de UK.

Por último, si se sigue tirando del hilo se puede ver que la empresa de la URL parece ser una tapadera para obtener datos, puesto que es un sitio web antiguo que no se ha actualizado o que anteriormente se utilizaba con este fin.

También se puede hacer un breve análisis del smishing, es decir, el phishing que se realiza a través de sms. Aquí tenemos un ejemplo de uno:

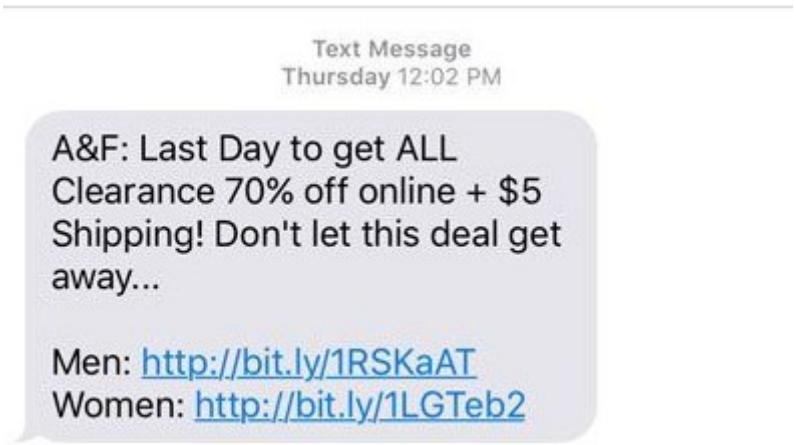



*Ilustración 11 Ejemplo de smishing*

En este caso, tenemos una “oferta” de un 70% y se puede ver algo que también es habitual y que permite “ocultar” la URL real, se trata de un “acortador” de URL, aunque la mayoría de estas utilidades acaban detectando el uso de esto para phishing y suelen borrar las URLs.

También hay otros casos, muy parecidos al de dpd simulando un servicio de paquetería, como este:

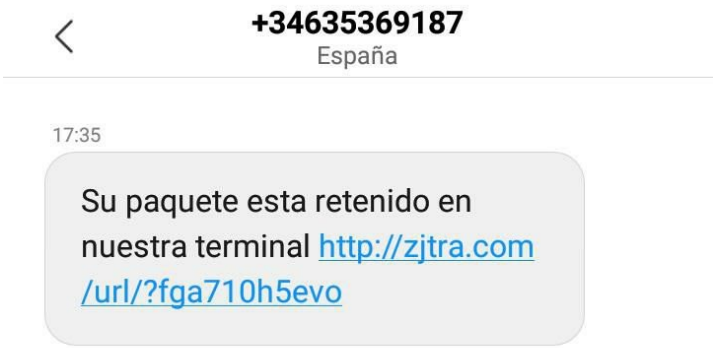



*Ilustración 12 Sms simulando un servicio de paquetería*

En este caso, aprovechándose de que este año ha aumentado el uso de servicios como Amazon, pues ha habido muchos casos de este tipo, donde te dicen que un paquete ha sido retenido o que ha habido un problema y te pasan una URL para comprobarlo.

Aquí si se realiza el mismo proceso que el caso anterior, se puede comprobar mediante Virustotal [20] que efectivamente es phishing, pero estas páginas suelen durar muy poco tiempo activas, por lo que la página ya no está activa.

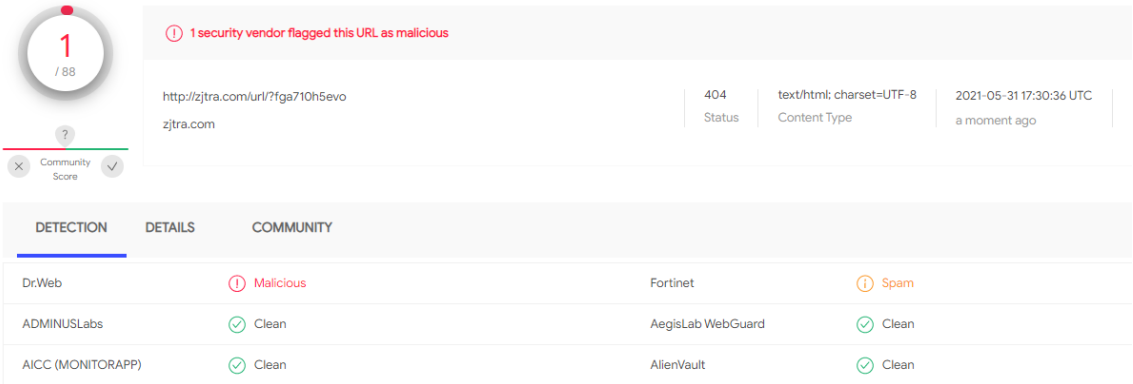



*Ilustración 13 Virustotal examinando la URL del SMS*

Con este pequeño y reducido análisis (se pueden encontrar más ejemplos en los anexos), se pretende comprobar que existen ciertas similitudes o “modus operandi” que se suele aplicar a la mayoría de este tipo de ataques.

Encontrar estos patrones es de mucha utilidad, tanto para ofrecerlo como ejemplo a gente no técnica como para la parte de IT de las empresas, ya que permite enseñar que es y como detectar este tipo de amenazas.

En particular, se debe tener especial cuidado con:

- **El remitente:** No es alguien conocido o intenta parecer que, si lo sea con pequeños cambios gramaticales, suele tener un dominio poco utilizado o este no concuerda con el correo.

- **El contenido del mensaje:** Intenta llamar la atención del receptor, provocando una sensación de urgencia o requiriendo acciones rápidas (ofertas que expiran en X tiempo, bloquear trasferencias inmediatas, problemas servicio de paquetería, etc.)

- **El link y la URL de esta:** Suele esta oculta en texto con hipervínculo o acortada, si la examinamos veremos que no suele tener que ver con el mensaje o incluso que intenta copiar la URL del sitio objetivo. También suelen utilizarse dominios extranjeros o poco comunes, algo que nos debe llamar la atención.

- **Errores gramaticales:** Es muy habitual encontrar errores gramaticales graves e incluso encontrar errores de contexto, es algo habitual en este tipo de mensajes.

- **Situaciones inverosímiles:** Muchas veces también suelen ser mensajes donde es explican situaciones que no encajan o ofrecen cosas que no hemos requerido. Por ejemplo, una firma de un banco que no es el nuestro o la compra de un terreno en un país lejano.

Por último, también hay que remarcar algunos aspectos que a veces no nos parecen tan graves, pero que ayudan en gran medida a evitar este tipo de problemas con el phishing, estos puntos son:

- **Diferenciar entre lo corporativo y lo personal:** No utilizar mails o teléfonos de la empresa en el ámbito personal y a poder ser evitar introducirlos en todos sitios, puesto que esto reducirá de manera visible la cantidad de mails o SMS fraudulentos y en gran medida ayudará a bajar el riesgo de ser objetivo de este tipo de prácticas.

- **Doble confirmación:** Durante esta época se ha estado trabajando mucho en remoto, esto ha hecho mucho daño, puesto que es más complicado confirmar cara a cara las informaciones recibidas, pero esta práctica debe seguir haciéndose, de forma que si se recibe un mail sospechoso suplantando a alguien hablar con esta persona para confirmarlo.

- **Utilizar herramientas externas:** Herramientas como extensiones o antivirus nos permiten a reducir el peligro ante este tipo de amenazas, hoy en día existen una gran cantidad de herramientas que permiten ayudar al usuario, como por ejemplo extensiones para navegadores como pueden ser, Malwarebytes Browser Guard, Privacy Badger o HTTPSeverywhere son simples extensiones de navegador que permiten mejorar nuestra seguridad de una forma simple y eficaz.
-
- **Reportar el phishing:** En la medida de lo posible, siempre es de ayuda reportar este tipo de cosas, tanto en el entorno corporativo al departamento correspondiente o marcando como spam el correo que nos llega a nuestras direcciones de correo personales, esto es de gran ayuda a la hora de crear grandes redes de datos que permitan tanto facilitar la identificación como su detección temprana.

Teniendo en cuenta estos simples puntos, se hace mucho más fácil encontrar correos o SMS fraudulentos. Aunque a veces puede resultar complicado, ya sea porque la plantilla del mail está muy bien hecho y copia a la perfección uno legítimo, o porque puede que si estemos esperando un paquete de la empresa X, pero si se examina y lee detenidamente siempre es posible encontrar uno de estos puntos en los correos o SMS, muy parecido al proceso mostrado anteriormente, donde los conocimientos técnicos necesarios son mínimos y de una manera bastante lógica se puede llegar a una conclusión clara sobre el correo o sms examinado.

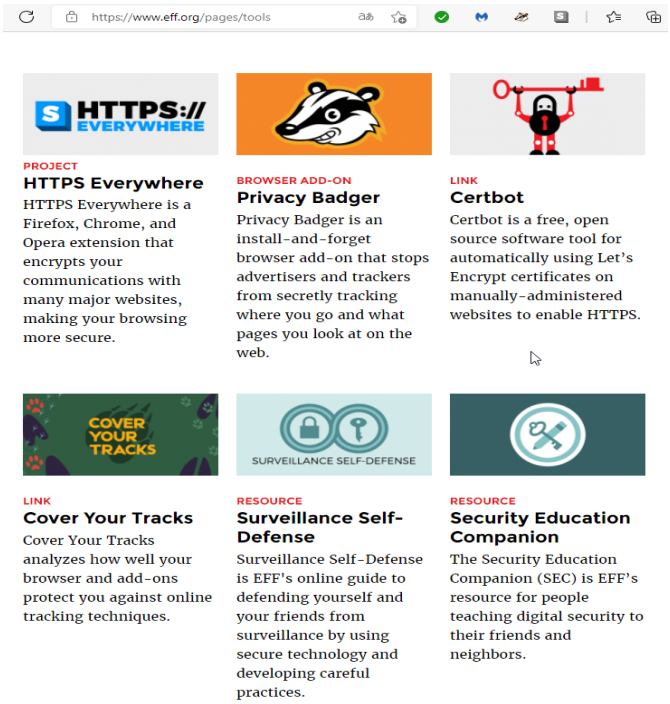



*Ilustración 14 Algunas de las herramientas mencionadas de EFF*

# 6. Comparación de herramientas

Existen diferentes tipos de herramientas para combatir el phishing, pero tras los resultados obtenidos en la encuesta realizada, queda claro que un punto clave para combatir la amenaza que supone el phishing es el entrenamiento, concienciación y aprendizaje sobre este tipo de amenazas.

Para este punto concreto existen una serie de herramientas que permiten realizar lo que se conoce como “campañas de phishing”. Estas herramientas permiten de una manera configurada entrenar a los usuarios sobre este tipo de amenazas, de forma que se pueden realizar diferentes envíos masivos de correos de phishing sobre una empresa, serán correos inocuos pero que permitirá saber tanto el nivel de desempeño del personal, como el efecto que tendría este tipo de ataques sobre una empresa.

Para el análisis y comparación de estas se utilizará una selección de estas, se han escogido las más utilizadas, mirando siempre que se pueda a utilizar herramientas de código abierto y con alta capacidad de configuración.

## 6.1 Phishing frenzy

Url: https://github.com/pentestgeek/phishing-frenzy

Este proyecto proporciona casi todo lo necesario para poder realizar una campaña de phishing, no es complicada de entender y parece que funciona correctamente durante las pruebas realizadas.

Además de github, cuenta con una página web con bastante documentación sobre el funcionamiento, instalación e incluso incluye una sección de donde poner obtener diferentes templates para mails. Podemos obtener estadísticas sobre el uso de la aplicación, así como configurar muchas opciones como por ejemplo exportar a xml o pdf los resultados obtenidos de las campañas realizadas.

El principal problema de este proyecto es la falta de mantenimiento, puesto que ni la web ni el repositorio ha sido actualizado desde hace más de 3 años, si miramos el repositorio de templates lleva siete años sin modificación alguna, esto hace que el proyecto este sin soporte por parte de la comunidad y abandonado.

## 6.2 King phisher

Url: https://github.com/rsmusllp/king-phisher

Otro proyecto con multitud de opciones y que tiene un repositorio actualizado y mantenido correctamente por la comunidad.

Se pueden tanto realizar campañas, copiar páginas webs para realizar el phishing y también incluyen varias mejoras para los templates de mails. Algo

muy interesante de este proyecto es que tiene un repositorio donde tiene plugins que se pueden añadir tanto al cliente como al servidor.

Como puntos en contra de este proyecto la documentación no es tan completa como algunos otros proyectos, también es limitado en cuanto a interfaz grafica es algo complicada de entender, así como la instalación es algo más compleja y limitada que otros proyectos.

## 6.3 Mercure

Url: https://github.com/atexio/mercure

Proyecto interesante debido a que tiene muchas características: creador de campañas, templates, estadísticas, creador de landing pages, etc.

También tenían pensado en un futuro crear mejores gráficos, una API, training, etc. Pero tras revisar el repositorio se puede comprobar que el proyecto lleva varios años abandonado, también esta limitado ya que es necesario Docker para su uso y la documentación es escasa.

La interfaz gráfica es muy simple y bastante clara, pero limitada y con el repositorio archivado y solo read-only, el proyecto parece que no tendrá continuidad en un futuro.

## 6.4 Gophishing

Url: https://github.com/gophish/gophish

Proyecto muy completo, con mucha documentación e información al respecto, fácil de implementar y de poner a punto con varios sencillos pasos, tiene tanto templates, como campañas, clonador de páginas webs e incluso una API y una buena guía de desarrollo. Además, está bastante bien mantenido con actualizaciones recientes y una gran comunidad de soporte detrás del proyecto.

Como aspectos negativos carece de algunas funcionalidades que otros proyectos si tienen, aunque son características más adicionales que la funcionalidad en si, como por ejemplo las herramientas de “credentials harvesting” y “mail harvesting”

Para la elección de la herramienta se han tenido en cuenta muchas de las variables y características mostradas. En este caso concreto hay dos herramientas que se han descartado desde un inicio, que son la “Phishing frenzy” y la “Mercure”, a pesar de ser dos buenos proyectos y que tienen muy buenas características, estos dos proyectos llevan años sin recibir actualizaciones ni mantenimiento, por lo que se podrían considerar como abandonados. Esto podría acabar generando problemas a largo plazo, puesto que puedan salir muchos bugs o problemas derivados del código fuente, lo que implicaría o bien revisar por completo todo el código y corregir los problemas que vayan surgiendo durante su uso o empezar el proyecto de nuevo con una base sobre lo ya realizado.

De las dos que quedan para decidir, Gophishing es la que visualmente aporta más, ya que no solo aporta una interfaz gráfica mucho más intuitiva y visual, sino que además tiene la capacidad de generar reportes directamente desde la herramienta.

Por otro lado, es mucho más compatible que “King Phisher” y mucho más rápido y fácil de montar. Otro punto a su favor es que su documentación está mucho mejor detallada y hay mucha más cantidad de información sobre el proyecto.

En lo que respecta a King Phisher, es mucho menos intuitiva pero tiene algunas características de las que carece Gophishing, como el “credentials harvesting” o incluso alertas vía SMS.

Tras evaluarlas detenidamente y superponiendo los pros y los contras de cada una se escoge finalmente Gophishing para realizar las pruebas.

Para finalizar, tras ver posibles características que podrían faltarle a esta herramienta, se toma la decisión de implementar un script en Python que permita y dote a la herramienta de una funcionalidad para mejorar sus templates de los mails. De forma que a partir de esta herramienta se pueda recopilar información de utilidad sobre la víctima o página objetivo.

Como principales objetivos de recolecta de este script se definen:

- Logos, slogans y características de la empresa.
- Mails internos o corporativos, más sus patrones.
- Nombres de empleados y jerarquía
- Posibles eventos o información relevante actual sobre el objetivo.
- Creación o soporte para templates para mails con la información anterior.

| Herramienta | Templates | Campañas | Pluguins | Clonador de webs | Email Harvesting | Credentials Harvesting | Estadísticas |
|---|---|---|---|---|---|---|---|
| **Phishing frenzy** | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ |
| **King Phisher** | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| **Mercure** | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ |
| **Gophishing** | ✔ | ✔ | | ✔ | | | ✔ |

| Herramienta | Geolocalización | Documentación completa | Complejidad | Actualizado | Sistema operativos | API |
|---|---|---|---|---|---|---|
| **Phishing frenzy** | | ✔ | Baja | | Linux / Docker | |
| **King Phisher** | ✔ | | Media | ✔ | Linux | |
| **Mercure** | | | Media | | Docker | |
| **Gophishing** | | ✔ | Baja | ✔ | Linux / Mac / Windows | ✔ |

# 7. Script para creación de templates.

Como parte de este trabajo, se marcó como objetivo añadir alguna utilidad o mejora la herramienta escogida.

Para ello, se aporta un script para mejorar y crear templates a partir de las páginas objetivo. La utilidad principal de este script es obtener datos a partir de la página web de la empresa objetivo para poder crear templates "realistas" y a su vez útiles, puesto que el template será generado a partir de datos obtenidos de la misma página.

Esto permite y persigue dos objetivos clave, por un lado se obtiene un template realista para ser utilizado por la herramienta, por lo que será mucho más útil y verosímil a la hora de utilizarlo como entrenamiento para los mismos empleados de esta empresa y por otro lado se puede ver claramente que es lo que puede obtener un atacante de la página objetivo, dando lugar a posibles correcciones de contenido o incluso poder llegar a eliminar datos, que igual son irrelevantes o substituibles para evitar dar información de más a los atacantes, por ejemplo una lista amplia de mails de los empleados.

Para la creación del script se han utilizado varias técnicas típicas del *pentesting* de páginas web, estas técnicas son:

- **Fuzzering** [21]: Es una técnica que permite a base de prueba y error encontrar los diferentes paths o direcciones, en este caso, de una página web objetivo. De forma que permite saber la estructura de la página web y que subpáginas contiene, para poder luego procesar estas.
- **Web scraping** [22]**:** Es una técnica que permite obtener y extraer datos e información de una página web.

Utilizando estas dos técnicas, se puede obtener datos como los mails, nombres, logos, etc. Toda esta información acaba resultando de mucha utilidad a la hora de crear un template de los mails para phishing.

Para realizar el fuzzering, existen varias opciones, utilizar una de las herramientas existentes, como puede ser Dibuster o Wfuzz, pero para este trabajo se ha escogido crear un pequeño script en Python que realice esta función, de manera que sea personalizable y donde poder ir añadiendo más funcionalidades al complemento, esto generar un resultado ya sea un txt o json, de donde el script de web scraping podrá coger los paths de la URL objetivo.

Al realizar el script de web scraping al ser algo más complicado de implementar desde cero, como se pensaba realizar el script en Python se hizo una búsqueda de librerías de Python que pudieran realizar esto de manera autónoma y con una mínima configuración.

Las librerías que se tuvieron en cuenta a la hora de realizar el script son las siguiente:

- Pyspider (http://docs.pyspider.org/en/latest/)

- Beautiful Soup (https://www.crummy.com/software/BeautifulSoup/)
- Scrapy (https://scrapy.org/)

Aunque todas son igual de validas, se encontraron algunos problemas que determinaron cual era la más conveniente.

El primer filtro para eliminar una de las librerías era la cantidad de documentación, información y ejemplos que se podían encontrar, en lo que Pyspider parecía que tenía menos soporte de la comunidad y de donde costaba más encontrar información de gente que lo hubiera utilizado en un pasado, además el github de la herramienta llevaba casi un año sin actualizarse.

Scrapy es la que parecía que tiene más soporte de la comunidad y que parece ser estar más actualizada, aunque de Beautiful Soup tampoco costaba encontrar ejemplos e información al respecto.

Durante el proceso de pruebas se hicieron pruebas tanto con Scrapy como con Beautiful Soup, a pesar de que Scrapy parece tener mucho más potencial a largo plazo la curva de aprendizaje de la librería es bastante más elevada que las otras dos, por lo que hubiera requerido de mucho más tiempo aprender a utilizarla adecuadamente para obtener los resultados esperados del script. Por ello, acabo escogiéndose Beautiful Soup, que, aunque parece tener menos potencial es mucho más intuitivo el desarrollo con esta librería y su implementación en Python.

Hay que destacar que tampoco es una herramienta “fácil” pero si más intuitiva que las anteriores, puesto que muchas veces durante el desarrollo del pequeño script han aparecido errores o no se obtenían los resultados concretos de las búsquedas.

Por último, este último script se le ha integrado la API de gophishing, que realmente es muy fácil de utilizar y que permite modificar y crear directamente los templates desde el código en Python, para crearlos luego en la interfaz gráfica del programa, por lo que no es difícil su manejo además de la documentación y ejemplos que existen que ayudan tanto a realizar la implementación como a solventar los posibles errores que pueden ir surgiendo durante la implementación.

# 8. Estado actual y futuro del Script

Actualmente el script funciona, de tal forma que a partir de una URL puede obtener sus *paths*, estos pasan al script de web *scraping* que obtendrá, links, mails e imágenes de la página objetivo.

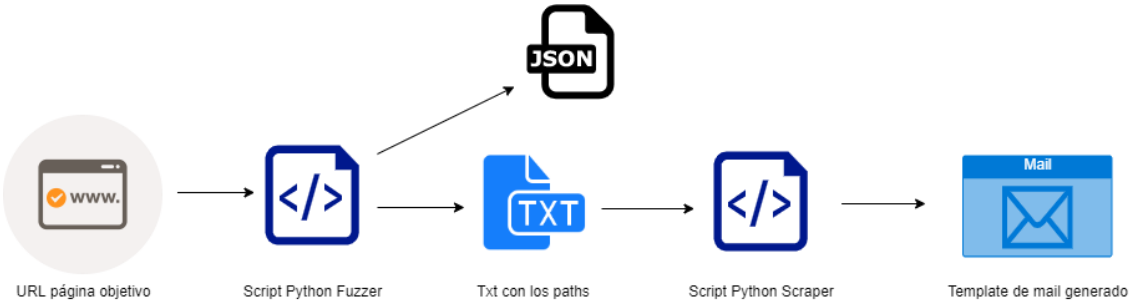



*Ilustración 15 Esquema del flujo de funcionamiento*

El script es funcional, aunque a veces no obtiene todos los datos que debería o como debería, ya que es bastante determinante el funcionamiento de la web objetivo o su esquema. Por ello se pretende en un futuro volver el script de Scraping más inteligente y que sea capaz de detectar más cantidad de información, así como cometer menos errores a la hora de obtener resultados visibles.

Se considera por tanto que se ha cumplido parcialmente el objetivo marcado sobre la creación del script que permita ayudar en la creación de los templates para las campañas de phishing. En un futuro, se pretende integrar los dos scripts en uno, así como mejorar y hacer más intuitivos estos. Es complicado definir una estructura sobre la que puedan trabajar bien puesto que muchas veces puede los errores de un lado llegan al otro, es decir, que puede que una parte este perjudicando a la otra, por ejemplo, a la hora de obtener resultados de los paths a veces aparecen paths extraños o que no el script del scraper no acaba de interpretar correctamente.

También se pretende mejorar su rendimiento, evitando que errores y mejorando la gestión de estos, puesto que actualmente no está implementada y a veces es complicado determinar porque no está funcionando correctamente el script.

Por último, otra parte a mejorar es el tema del templates puesto que actualmente solo se puede poner texto, ya que la API no soporta algunas cosas, como por ejemplo el traspaso de imágenes que debe realizarse a través de URLs, por lo que requiere subir estas a un servidor externo, que o bien podría implementarse de alguna forma o buscar una alternativa para poder crear mejores templates.

# 9. Conclusiones

El trabajo realizado da una clara visión sobre un aspecto actual que hay que mejorar, se trata de la educación en ciberseguridad.

Tras la encuesta y las conclusiones obtenidas durante la investigación, queda claro que una gran parte de la sociedad desconoce muchas de las amenazas que existen en Internet, concretamente, el phishing. Esto no solo supone un problema, sino que cuanto más pasan los años más grande es la brecha de conocimiento entre esta gente con perfiles no técnicos y los perfiles técnicos, lo que no solo empeora la situación, si no que permite ver claramente que cada vez será más complicado cubrir esa brecha de conocimiento.

Esto a simple vista no parece suponer un gran problema para algunos, pero a la larga supondrá un reto mayor para el campo de la ciberseguridad, puesto que los usuarios sin conocimientos básicos sobre ciberseguridad serán, cada vez más, el objetivo de los ciberdelincuentes puesto que será mucha más fácil engañar a esta gente o perfiles objetivo.

Es primordial poner remedio a esto, no solo en el ámbito laboral, dando charlas de concienciación, sino también a nivel escolar, pudiendo aplicar y enseñar ciberseguridad desde una edad temprana. Por otro lado, también es importante la investigación y desarrollo de herramientas que permitan llevar a cabo esta tarea de una manera mucho más simple y que también permita llegar a un público con mucho menos conocimientos técnicos de manera entendible.

Queda claro que cada año estas amenazas van a ir creciendo en número y complejidad, con la entrada en juego de la IA en los ciberataques el phishing podría acabar convirtiéndose en un problema de una gran envergadura, por ello es importante lo expuesto anteriormente, porque no solo supondrá un gasto cada vez mayor a las empresas y compañías, si no que cada vez tendrá un impacto mucho más grande en la comunidad y en el mundo en general. Es vital la inversión en formación, desarrollo e investigación aparte de hacer más visible el problema, puesto que actualmente no se cree que esto sea un problema como el que ya es, donde muchas veces usuarios de todo el mundo a diario sufren el acoso constante de SMS, mails, mensajes que crean el gran entramado del phishing y variantes, que más allá de ponerse soluciones se está llegando a un punto de ver como normal este tipo de acciones.

Por ello, con este trabajo he pretendido dar un poco de visibilidad al problema y poder aportar un granito de arena para combatir este tipo de prácticas.

# 10. Referencias


[1] W. Whitmore, «IBM,» 29 11 2020. [En línea]. Available: https://www.ibm.com/thought-leadership/institute-business-value/report/covid-19-cyberwar. [Último acceso: 15 Marzo 2021].

[2] It Reseller, «IT reseller,» 27 01 2021. [En línea]. Available: https://www.itreseller.es/seguridad/2021/01/seis-de-cada-10-cso-y-ciso-en-espana-han-visto-aumentar-los-ataques-de-phishing. [Último acceso: 2021 Enero 16].

[3] T. Kulikova, «Securelist (Kaspersky),» 15 02 2021. [En línea]. Available: https://securelist.com/spam-and-phishing-in-2020/100512/. [Último acceso: 2021 Febrero 22].

[4] C. Jiménez y R. Rivera, «Ciberseguridad del IoT: Un Análisis en Países de la Unión Europea,» *Revista Ibérica de Sistemas e Tecnologias de Informação,* nº E39, pp. 461-476, 2021.

[5] INCIBE, «Instituto Nacional de Ciberseguridad,» 2020. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/kit-concienciacion. [Último acceso: 19 02 2021].

[6] V. Chamorro y R. Rivera, «Twitter mining for multiclass classification events of traffic and pollution,» de *International Conference on Human Systems Engineering and Design: Future Trends and Applications*, Munich, 2019.

[7] C. Castillo, «BBVA,» 2020. [En línea]. Available: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/. [Último acceso: 25 02 2021].

[8] Kaspersky, «Kspersky,» 2020. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/spear-phishing. [Último acceso: 25 02 2021].

[9] Kaspersky, «Kaspersky,» 2020. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack. [Último acceso: 25 02 2021].

[10] Colaboradores de Wikipedia, «Wikipedia Ingeníeria Social,» 2020 11 19. [En línea]. Available: https://es.wikipedia.org/w/index.php?title=Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)&oldid=131047316. [Último acceso: 2021 Marzo 24].

[11] Avast Academy Team, «Avast Academy, Ingeniería Social,» 2021 02 23. [En línea]. Available: https://www.avast.com/es-es/c-social-engineering. [Último acceso: 2021 Marzo 24].

[12] Kaspersky, «Kapersky "Ingeniería social",» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering. [Último acceso: 2021 Marzo 24].

[13] R. Rivera, L. Pazmiño, F. Becerra y J. Barriga, «An Analysis of Cyber Espionage Process,» de *Developments and Advances in Defense and Security. Proceedings of MICRADS 2021*, Cartagena, 2021.

[14] M. Sebastián, R. Rivera, P. Kotzias y J. Caballero, «AVclass: A Tool for Massive Malware Labeling,» de *International symposium on research in attacks, intrusions, and defenses*, 2016.

[15] P. Kotzias, S. Matic, R. Rivera y J. Caballero, «Certified PUP: abuse in authenticode code signing,» de *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[16] R. P. Rivera-Guevara, Deteccion y Clasificacion de Malware con el Sistema de Análisis de Malware Cuckoo, UNIR, 2018.

[17] R. R. Guevara, Tools for the detection and analysis of potentially unwanted programs, (Doctoral dissertation, Tesis doct. Nov. de 2018. doi: 10.20868/UPM. thesis.53395), 2018.

[18] R. Rivera, P. Kotzias, A. Sudhodanan y J. Caballero, «Costly freeware: a systematic analysis of abuse in download portals,» *IET Information Security,* vol. 13, nº 1, pp. 27-35, 2019.

[19] R. R. Guevara, ANÁLISIS DE CARACTERÍSTICAS ESTÁTICAS DE FICHEROS EJECUTABLES PARA LA CLASIFICACIÓN DE MALWARE, UNIVERSIDAD POLITÉCNICA DE MADRID, 2014.

[20] C. G. Amaya, «WeLiveSecurity,» 6 10 2017. [En línea]. Available: https://www.welivesecurity.com/la-es/2017/10/06/trucos-mitos-virustotal/. [Último acceso: 01 05 2021].

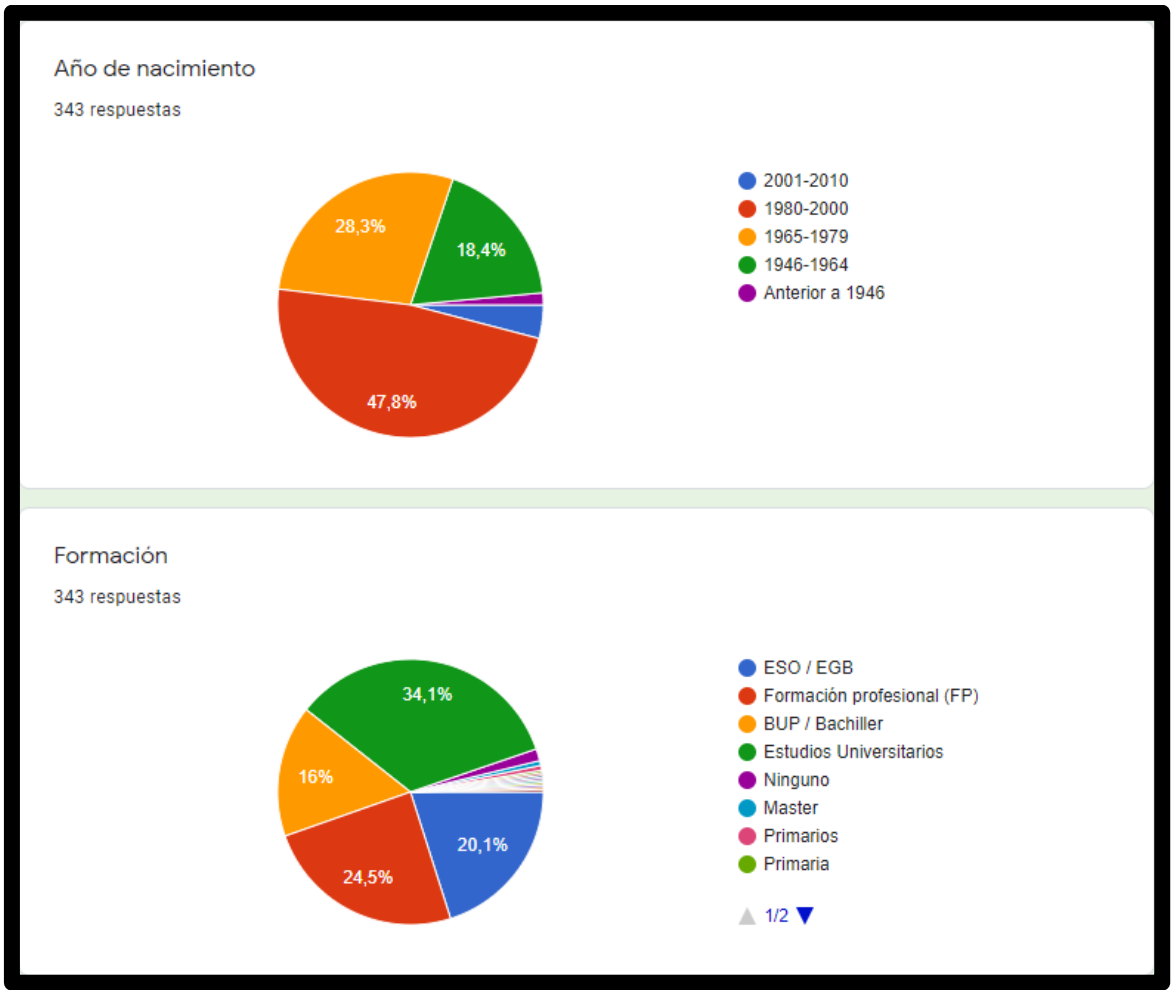
[21] Wikipedia, «Fuzzing,» 10 4 2021. [En línea]. Available: https://en.wikipedia.org/wiki/Fuzzing. [Último acceso: 18 04 2021].

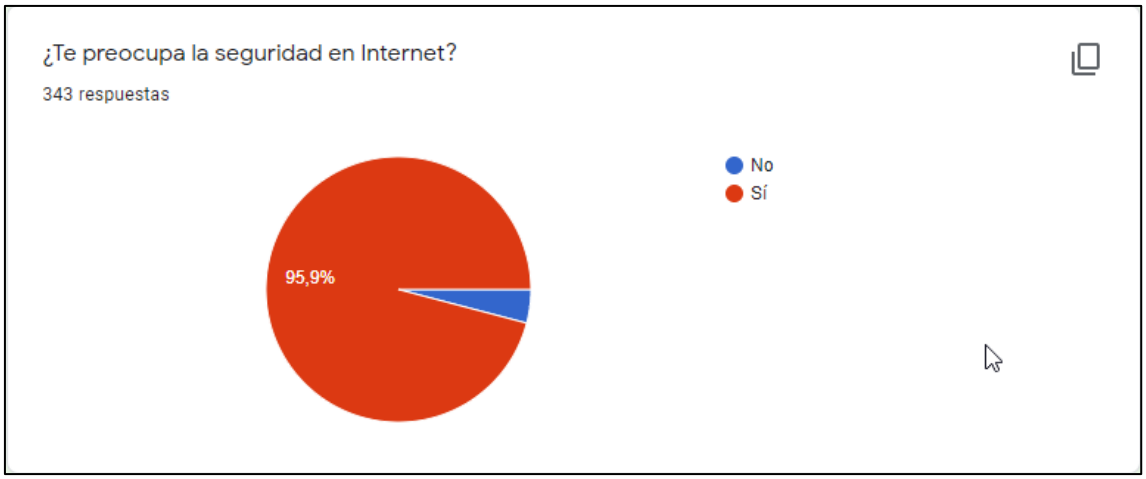
[22] IONOS, «IONOS digital guide,» 10 09 2020. [En línea]. Available: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/que-es-el-web-scraping/. [Último acceso: 05 04 2021].

[23] L. Pazmiño, F. Flores, L. Ponce, J. Zaldumbide, V. Parraga, B. Loarte, G. Cevallos, I. Maldonado and R. Rivera, "Challenges and Opportunities of IoT Deployment in Ecuador," in *2019 International Conference on Information Systems and Software Technologies (ICI2ST)*, Quito, 2019.

# 8. Anexos

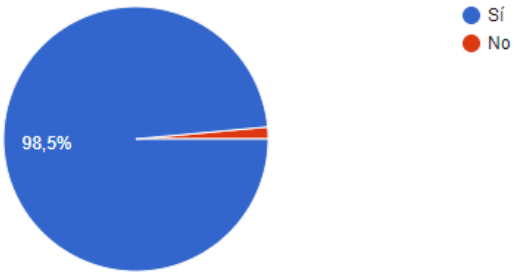
## 8.1 Anexo 1 Datos completos de las encuestas



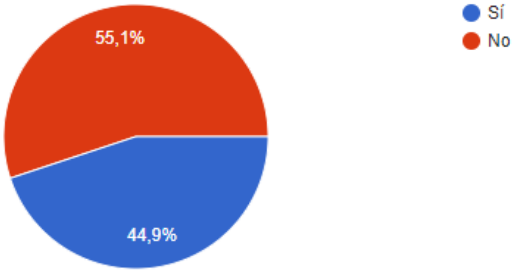
¿Crees que se debería enseñar más sobre seguridad informática básica?

343 respuestas



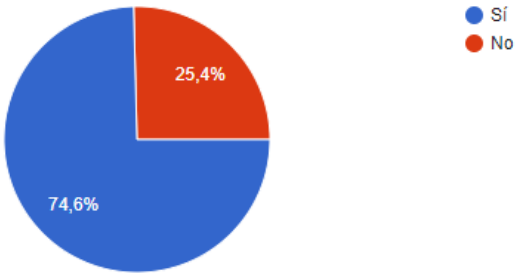

¿Sabes que es el phishing?

343 respuestas



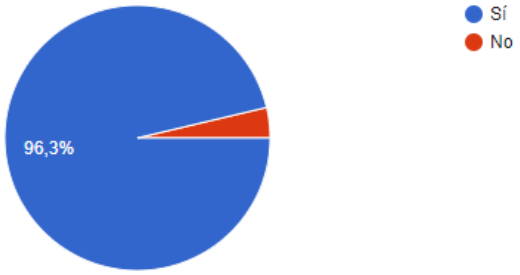

Tras leer la definición ¿Ahora sabes que es el phishing o sabrías reconocerlo?

189 respuestas



¿Crees que te falta formación y conocimientos de seguridad informática en tu día a día?

189 respuestas

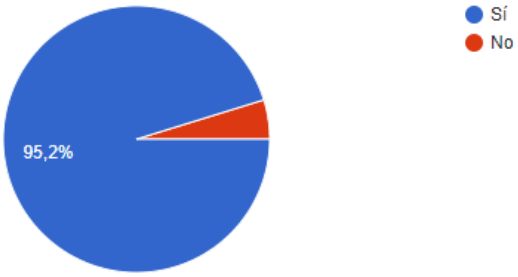



¿Te dan algún curso o recomendación en tu Escuela/Instituto/Trabajo, para prevenir este tipo de estafas en Internet?

189 respuestas

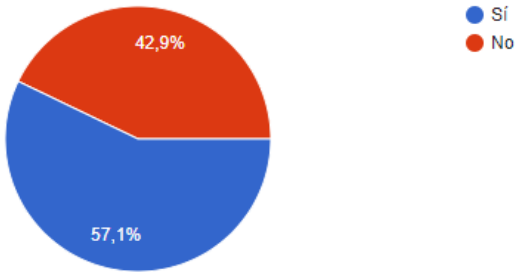

¿Crees que cada vez es más complicado distinguir estafas en Internet?

189 respuestas



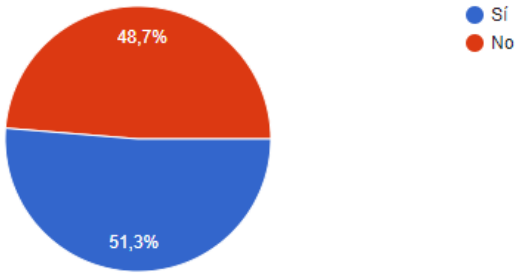
¿Conoces a alguien que haya tenido problemas por el phishing?

154 respuestas



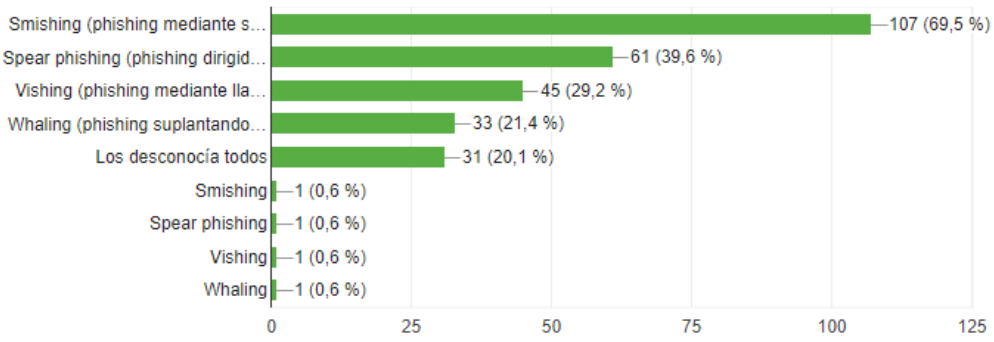

¿Sabes como hay que actuar si algún día te llega a suceder?

154 respuestas



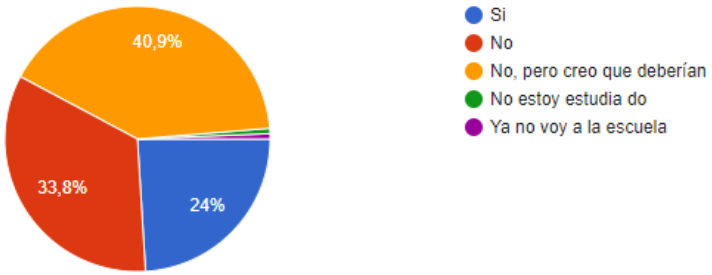

Marca cuales de estos tipos conoces

154 respuestas



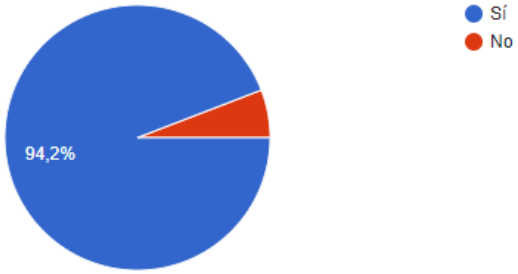
¿Te dan algún curso o recomendación en tu Escuela/Instituto/Trabajo para prevenir este tipo de estafas en Internet?

154 respuestas




¿Crees que cada vez es más complicado distinguir estafas en Internet?

154 respuestas

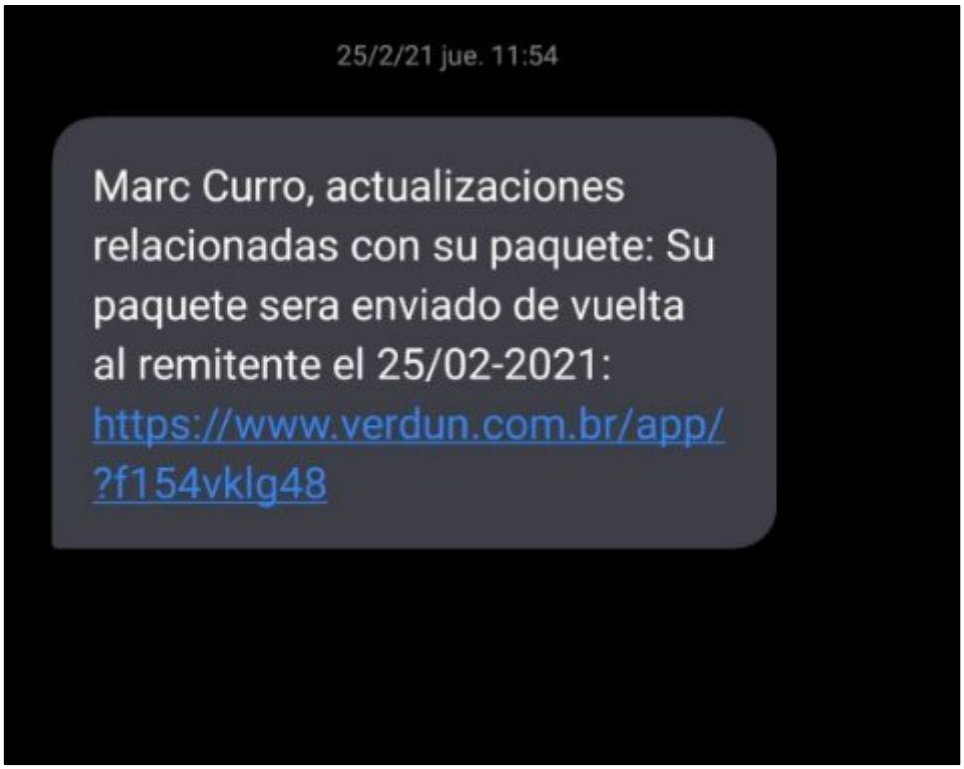


## 8.2 Anexo 2 Muestra de Phishing/Smishing recolectados



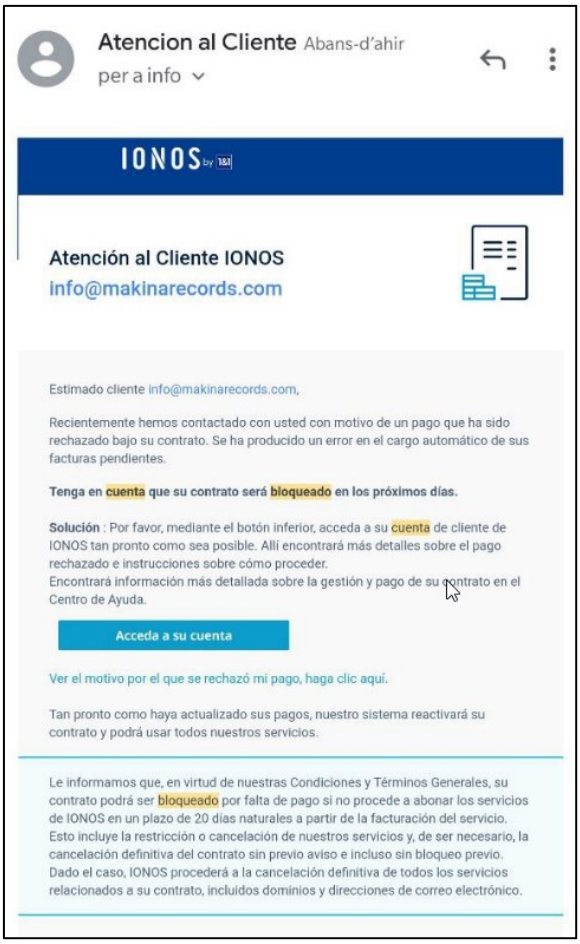
+34664685283
España
16/2/21 mar. 19:35
FedEx: Tu envio esta por llegar, rastrealo aqui: https://demirayasansor.com.tr/fedex/?tflfeeckaf


+34601357211
España
2/3/21 mar. 16:11
SEUR: envio 402922 de MOR BER FASHION SL no entregado. Direccion desconocida. Programe entrega alternativa en https://nen.vacad.net/pkg/?iv7rn17mo1


25/2/21 jue. 11:54
Marc Curro, actualizaciones relacionadas con su paquete: Su paquete sera enviado de vuelta al remitente el 25/02-2021: https://www.verdun.com.br/app/?f154vklg48


+34664160794
España
16/2/21 mar. 16:43
FedEx: Tu envio esta por llegar, rastrealo aqui: http://www.medigochile.cl/fedex/?dbvbz265qp


+34610011967
España
16:25
Estimado Chiki, tenemos su paquete en la cola. Direccion: Hojiblanca: https://alercehistorico.cl/pkg/?r1f75recw0


Atencion al Cliente Abans-d'ahir
per a info
IONOS by 1&1
Atención al Cliente IONOS
info@makinarecords.com
Estimado cliente info@makinarecords.com,
Recientemente hemos contactado con usted con motivo de un pago que ha sido rechazado bajo su contrato. Se ha producido un error en el cargo automático de sus facturas pendientes.
Tenga en cuenta que su contrato será bloqueado en los próximos días.
Solución : Por favor, mediante el botón inferior, acceda a su cuenta de cliente de IONOS tan pronto como sea posible. Allí encontrará más detalles sobre el pago rechazado e instrucciones sobre cómo proceder.
Encontrará información más detallada sobre la gestión y pago de su contrato en el Centro de Ayuda.
Acceda a su cuenta
Ver el motivo por el que se rechazó mi pago, haga clic aquí.
Tan pronto como haya actualizado sus pagos, nuestro sistema reactivará su contrato y podrá usar todos nuestros servicios.
Le informamos que, en virtud de nuestras Condiciones y Términos Generales, su contrato podrá ser bloqueado por falta de pago si no procede a abonar los servicios de IONOS en un plazo de 20 días naturales a partir de la facturación del servicio.
Esto incluye la restricción o cancelación de nuestros servicios y, de ser necesario, la cancelación definitiva del contrato sin previo aviso e incluso sin bloqueo previo.
Dado el caso, IONOS procederá a la cancelación definitiva de todos los servicios relacionados a su contrato, incluidos dominios y direcciones de correo electrónico.

D

DPD UK - Next Day Delivery <tnrogsqr08829ulneidj@telenet.be
>
Lun 30/11/2020 19:34
Para: [redacted]

Hello [redacted]

Never miss a parcel delivery again

Your parcel number 09139501230

We tried to deliver your parcel today but you weren't in or there was no safe place to leave it.

Your action is required. If this item is unclaimed by the return date, then it will be returned to sender.

The first and second delivery attempt was free of charge

To schedule a new delivery, a shipping fee must be paid.

Reschedule parcel delivery >

(Please don't reply to this email.)

News:

Send from only £3.99
Drop off or collect your parcel from your nearest shop contact- free
Our overseas service offers unbeatable, flexible solutions for all your delivery and logistics needs for Europe and the rest of the world.

[ wleetpzfprthhjoctwod ]

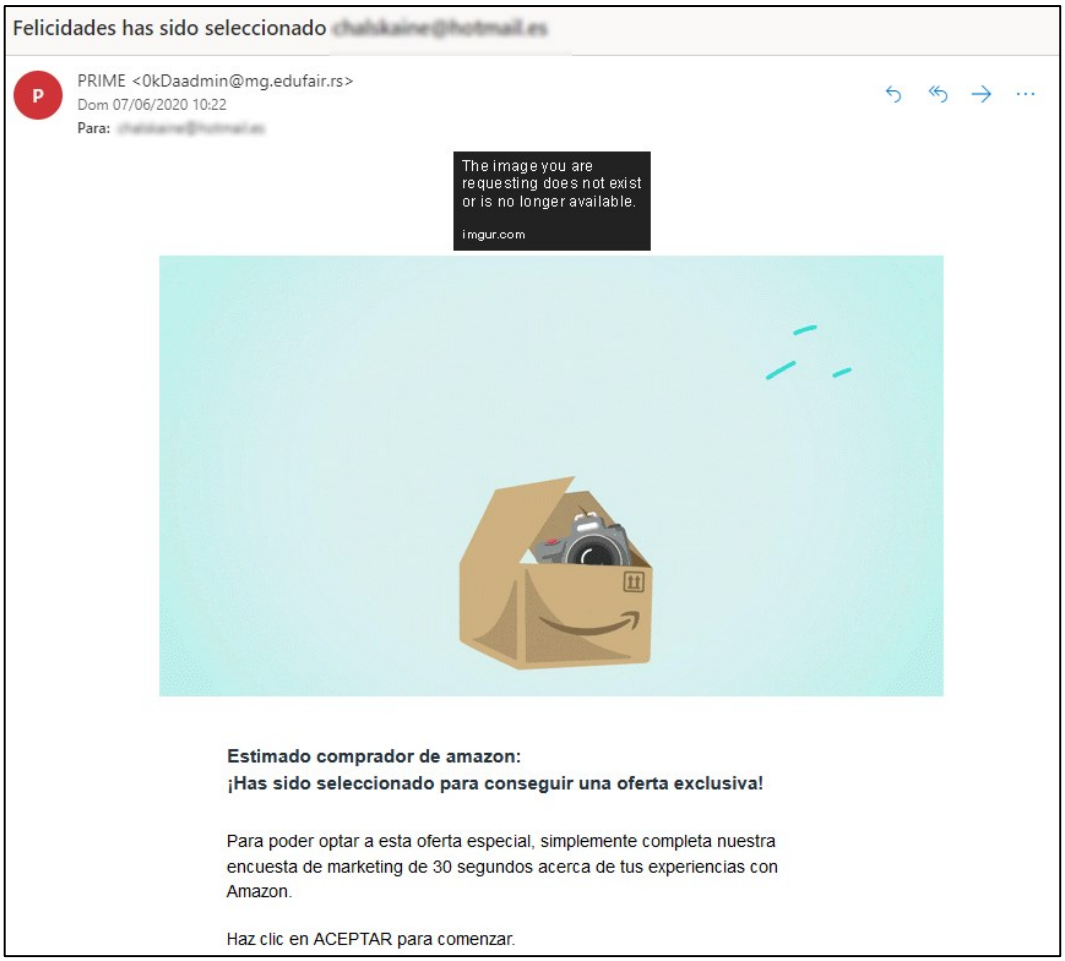
*This is an automated email sent to charly_8-93@hotmail.com, please do not reply.

DPD News

Querido cliente Lidl

EA

Emieza Ahora!! <E8WMinfo@gellifique.co.uk>
Mié 11/11/2020 15:23
Para: [redacted]


Felicidades has sido seleccionado
PRIME <0kDaadmin@mg.edufair.rs>
Dom 07/06/2020 10:22
Para:
The image you are requesting does not exist or is no longer available.
imgur.com
Estimado comprador de amazon:
¡Has sido seleccionado para conseguir una oferta exclusiva!
Para poder optar a esta oferta especial, simplemente completa nuestra encuesta de marketing de 30 segundos acerca de tus experiencias con Amazon.
Haz clic en ACEPTAR para comenzar.


[Emergencia]: lea este correo electrónico - DE# 2132381517
Bankia <Serviciobankia2132381517@void.es>
Mar 21/01/2020 10:23
Para:
[Urgente].txt
35 KB
Responder
Reenviar

SN

Sweet Nastya <damonnqeviaz@outlook.com>
Sáb 04/01/2020 19:03
Para: [redacted]

Bienvenida!;)
Espero, te sientes muy bien? Ha tomado la decision mas cerca conocer a nosotros.
Busco seguro las relaciones en las redes. Me llamo Nastya. Mi optimistico y simple la mujer. Conduzco una alimentacion correcta y la ausencia de las malas costumbres. No tengo la dependencia de nicotina y no bebo las bebidas alcoholicas. Me quiero ocuparse del deporte. En caso de que tienes el interes en la continuacion nuestro de la comunicacion, responde. Si es interesado, puedo escribirte mas la informacion. Nunca no estaba casado y no tengo a ninos. La peticion pequena, cuenta mas sobre. Sueno conocer contigo y conocerte te mas vale. Si tienes la posibilidad, por favor, han llegado a mi tuyos la foto. Y luego sujetare a ti mis las fotografias.
Esperare tu respuesta con grande por la impaciencia.
Con los mejores deseos, Anastasia.

Aviso importante [ID-202338]

BS

Banco Santander <info-lxlela@biurrun.de>
Sáb 30/11/2019 13:31
Para: [redacted]

Santander

Asunto : Su tarjeta será suspendida

Remitente : Servicio al cliente.

Estimado Cliente ,

Estamos teniendo problemas para verificar la información de su tarjeta de crédito.

Lo invitamos a corregir este problema haciendo clic en el enlace de abajo y siguiendo las instrucciones :

**Haga clic aqui,y iniciar sesion en su cuenta**

Banco Santander, con domicilio social en calle Pintor Sorolla Nº8, 46002 Valencia, y CIF A-