ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Máster

Elaboración de una herramienta de concienciación para dispositivos Android para evitar ser víctima de phishing

(Development of an awareness tool for Android devices to avoid being a victim of phishing)

Para acceder al Título de

Máster Universitario en Ingeniería de Telecomunicación

Autor: José Domingo Castro Crespo

Septiembre – 2022

Resumen

Desde el comienzo del siglo XXI, el Internet se ha consolidado en la sociedad. Esto se debe a que los ordenadores personales y las tarifas de Internet de las compañías móviles se han vuelto más accesibles y, en gran medida, por la irrupción de los dispositivos móviles, logrando que la gran mayoría de la población esté totalmente conectada. Además, la pandemia por COVID-19 del año 2020 causó que las personas fuesen dependientes del Internet debido al teletrabajo y a la cuarenta, ya que esta era la única forma posible de conectarse al mundo.

Sin embargo, Internet también tiene sus peligros. Muchos ciberdelincuentes se han visto beneficiados por el aumento de los usuarios conectados a la red, ya que muchos de ellos son personas mayores o que nunca la habían utilizado y desconocen los peligros que esta contiene. Además, el mundo laboral ha basculado al teletrabajo lo que ha facilitado la tarea de los cibercriminales para atacar a las empresas. Por estos motivos, los ciberataques han aumentado considerablemente en los últimos años.

Por tanto, con este trabajo se busca concienciar a las personas de los peligros que se ocultan en Internet y propiciar las herramientas necesarias para evitar ser víctimas de un ciberataque. En concreto, este trabajo se centra en uno de los ciberataques más comunes: el phishing.

Abstract

Since the beginning of the 20th century, the Internet has consolidated in society. This is due to the increase in the accessibility of personal computers and internet rates and the appearance of mobile devices, achieving that most of the population is always connected to the network. In addition, the COVID-19 pandemic of 2020 caused people to be dependent on the Internet due to telework and quarantine, since this was the only possible way to connect with the world.

However, Internet also has its dangers. Many cybercriminals have benefited from the increase of users connected to the network, since many of them are old people or have never used it before and are unaware of the dangers it contains. In addition, the workplace has shifted to telework, which has made it easier for cybercriminals to attack companies. For these reasons, cyberattacks have increased considerably in recent years.

Therefore, this work seeks to raise people's awareness of the dangers that are hidden on the Internet and provide the necessary tools to avoid being victims of a cyberattack. Specifically, this work focuses on one of the most common cyberattacks: phishing.

Índice

Lista de figuras

Lista de tablas

Acrónimos

CSIRT	Equipo de Respuesta ante Emergencias Informáticas
DDoS	*Distributed Denia lof Service*
DNS	*Domain Name System*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
INCIBE	Instituto Nacional de Ciberseguridad en España
SEC	Sistema Estadístico de Cibercriminalidad
SMTP	*Simple Mail Transfer Protocol*
UNODC	*United Nations Office on Drugs and Crime*
URL	*Uniform Resource Locator*
VPS	*Virtual Private Server*

Capítulo 1. *Introducción*

La criminalidad siempre ha existido en la sociedad. En todas las etapas de la historia han existidos delincuentes que se dedicaban a realizar actos criminales con el fin de obtener unos beneficios de forma fácil. Conforme la tecnología ha ido evolucionando, la sociedad se ha ido adaptando a ella, consiguiendo una vida cada vez más cómoda. Sin embargo, los criminales también se han adaptado a este avance tecnológico, consiguiendo nuevas herramientas o encontrando nuevas vulnerabilidades en la sociedad para hacer que sus ataques sean más efectivos.

La tecnología más disruptiva de los últimos tiempos es el internet. Esta tecnología junto a la popularización y el fácil acceso a los ordenadores personales provocó un cambio completo en la forma de vivir y de interactuar unas personas con otras. Gracias al internet, las personas pueden compartir información o comunicarse desde cualquier parte del mundo. Además, está tecnología ha ido evolucionando hasta permitir compras online, retransmisiones en vivo, almacenar grandes cantidades de datos en la nube, comunicaciones instantáneas de mensajería, voz o video, entre otros muchos servicios.

Asimismo, los cibercriminales se han adaptado a las nuevas tecnologías, encontrando nuevas formas de estafar o robar, entre otros crímenes, a personas que están navegando por la red. Los criminales han encontrado en internet una gran cantidad de vías y herramientas para poder atacar a otras personas. Además, ya no necesitan estar en el lugar de la víctima, sino que, como el internet es una tecnología global, pueden tener como objetivo a cualquier persona del mundo por el simple hecho de estar conectado a internet.

En los comienzos del internet, un ciudadano promedio no tenía acceso a este, ya que su uso era más exclusivo, no ofrecía muchos servicios a la sociedad en general y tener un ordenador personal no era tan accesible como lo es hoy en día. El avance en la informática, la reducción de los precios de los ordenadores personales y la facilidad actual que hay para conectarse a internet, hace que en los últimos años el número de cibernautas haya aumentado considerablemente. Además, hay que tener otros factores en cuenta como la pandemia por COVID-19 en el año 2020. Esta pandemia causó que aumentase la cantidad de teletrabajo y la cantidad de tráfico de internet, ya que la gente no podía abandonar sus casas. Esto ocasionó que muchos usuarios inexpertos o inconscientes de los peligros del internet pasase más tiempo en la red, aumentando la probabilidad de recibir un ciberataque.

Navegar por internet no es completamente seguro, ya que un mal uso de este puede causar muchos problemas. Muchas veces los cibercriminales se aprovechan del desconocimiento de las personas que no están muy familiarizados con esta tecnología, ya sea por su edad o que nunca han tenido la oportunidad de utilizarla, para atacarlas y obtener beneficios a partir de ellas de forma ilícita. Pero no solo se aprovechan de la ignorancia de la gente, ya que también se aprovechan de errores en fallos en el código de los programas o los bajos niveles de defensa que

tienen algunos servicios para encontrar un agujero y atacar a empresas o instituciones gubernamentales.

Solo en el año 2020, hubo 316 millones de nuevos usuarios de internet (Figura 1). Otro factor importante para el aumento de usuarios en internet es la aparición de los dispositivos móviles, ya que los *smartphones* permiten el acceso a internet desde cualquier lugar. En el año 2020 incrementó en 93 millones el número de personas con un teléfono inteligente propio (Figura 1). Esto es una buena noticia, pero a su vez también es una nueva vía para nuevas posibles formas de ataque.

Por estos motivos, es muy importante concienciar y enseñar a la gente de los peligros ocultos en internet para evitar posibles estafas, robos de identidad o de dinero, entre otros ciberataques, para reducir al máximo posible el número de víctimas en el ciberespacio. Al igual que es importante concienciar a los individuos, también es importante persuadir a las empresas o instituciones gubernamentales en aumentar su ciberseguridad pare evitar posibles ataques. Por ejemplo, realizar copias de seguridad de la información, invertir parte de su presupuesto en ciberseguridad y la formación de sus empleados en este campo.

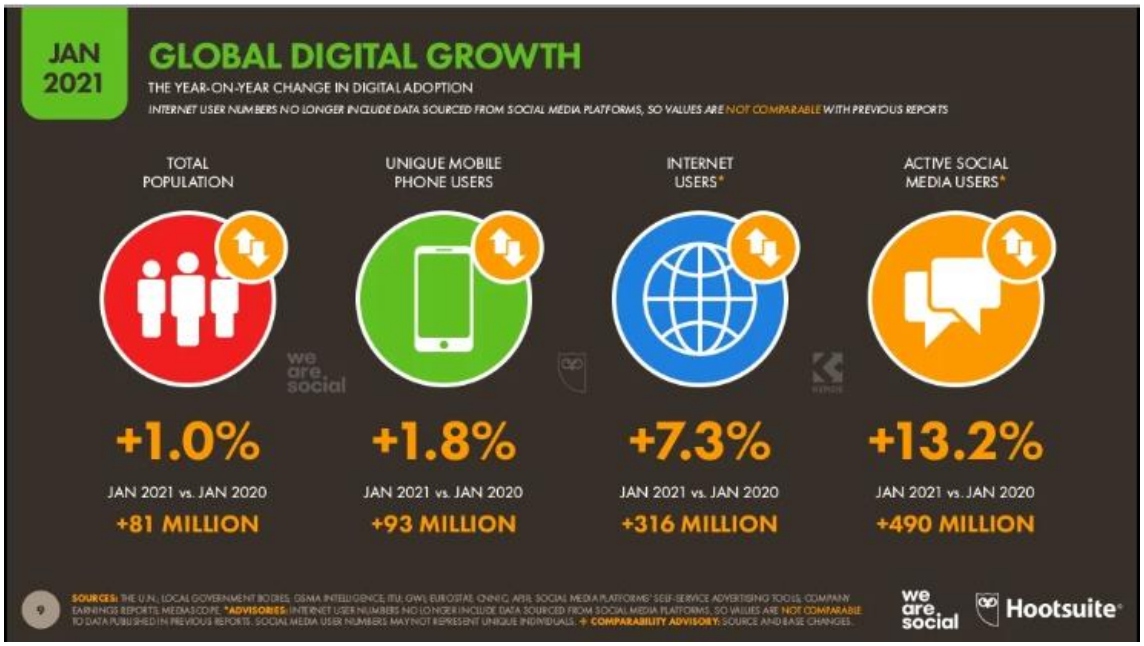


Figura 1: Aumento de usuarios en diferentes tecnologías a nivel mundial en 2020 [1].

1.1 Motivación

Actualmente, el mundo se encuentra en la sociedad de la información que se caracteriza por el uso de las tecnologías de la información y de la comunicación (TIC) para poder intercambiar datos y permanecer constantemente comunicados con el resto de la sociedad tanto a nivel laboral como en el personal. Esta sociedad es posible gracias a la mayor tecnología disruptiva de los últimos tiempos: el Internet. Gracias a internet es posible compartir información y comunicarse con cualquier persona de cualquier parte del mundo de una forma rápida y sencilla, necesitando solo un dispositivo capaz de conectarse a la red.

La posibilidad de poder estar conectado a la red ha venido acompañada de una gran cantidad de ventajas, pero también oculta muchos peligros. Muchos de los nuevos usuarios, muchos de ellos son personas mayores o personas de países subdesarrollados, son totalmente desconocedores de los peligros que se encuentran en Internet, convirtiéndose en blancos fáciles para los ciberdelincuentes. Pero no solo los nuevos usuarios son vulnerables a los ciberataques, sino que cualquier dispositivo conectado lo es. En general, la mayoría de los usuarios son desconocedores de estos peligros o consideran que a ellos nunca le sucederá. Por este motivo, no se prestan las medidas de seguridad necesarias para prevenir este tipo de ataques hasta que se ha sido víctima de uno, causando grandes pérdidas de información o económicas a las víctimas.

En los últimos años, los ciberataques han crecido rápidamente. El ciberataque más común y del cual cualquier usuario puede ser víctima es el *phishing*. Los cibercriminales se aprovechan del exceso de confianza y del desconocimiento de las personas para suplantar la identidad de otra persona u organismo para que la víctima entregue sus datos. Con estos datos podrían acceder a la cuenta bancaria o al correo corporativo de la víctima, causando muchos problemas.

Por tanto, el objetivo de este TFM es enseñar a las personas los peligros que se encuentran en Internet y concienciarles para que se tomen buenas prácticas de ciberseguridad con el fin de evitar ser víctima de un ciberdelincuente. Además, este trabajo se centrará en el phishing, ya que se trata de uno de los ciberataques más sufridos por la sociedad. El phishing puede ser evitado con campañas de formación y concienciación que serán el objetivo de este trabajo y se implementarán mediante el uso de una herramienta.

1.2 Estructura

Este documento está organizado en siete capítulos en los que se recoge la siguiente información:

- En el primer capítulo se explica de manera breve el contexto en el que se encuentra este trabajo en el ámbito de la cibercriminalidad y la motivación de la realización de este.
- En el segundo capítulo se expone la historia de la cibercriminalidad, los ciberataques más comunes y sus estadísticas en España durante el año 2020.
- En el tercer capítulo se centra en un tipo de ciberataque en concreto: el phishing. Se explica lo que es, las técnicas que se utilizan para llevarlo a cabo y el proceso de realización de una campaña de phishing. Además, de las temáticas más utilizadas.
- En el cuarto capítulo se explican los tipos de phishing que existen.
- En el quinto capitulo se explican los recursos accesibles en internet para contrarrestar el phishing. Además, se analizan campañas de phishing que ya se han realizado y los efectos que han tenido.
- En el sexto capítulo se elabora una herramienta de formación y concienciación anti-phishing.
- En el último capítulo de este documento, se exponen las conclusiones a las que se ha llegado durante la elaboración de este trabajo y las posibles líneas futuras que se pueden realizar.

Capítulo 2. *La cibercriminalidad*

La cibercriminalidad o ciberdelincuencia está muy presente en la sociedad global actual, generando grandes pérdidas económicas a personas, empresas e instituciones. La UNODC (Oficina de las Naciones Unidad contra la Droga y el Delito) define la cibercriminalidad como "un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito." [2]. La ciberdelincuencia tiene las ventajas frente al delito tradicional de que no tiene barreras físicas y se puede realizar de forma más rápida y sencilla.

Los expertos consideran que el primer ciberdelito se realizó sobre una red de telegrafía en el año 1834 [3]. Los atacantes lograron vulnerar la seguridad del sistema y lograron obtener información sobre el mercado financiero y bancos. Durante la segunda mitad del siglo XX los ataques por cibercriminales aumentaron y se centraron en ataques a los teléfonos, dando lugar al origen del pirateo telefónico o *phreaking*. El primer ataque de este tipo fue en Estados Unidos en el año 1950. El atacante logró imitar el sonido del código emitido por los sistemas telefónicos para establecer la comunicación. De esta forma, el atacante podía hacer llamadas telefónicas gratuitas haciéndose pasar por un empleado. Una década más tarde, se crackeo la primera contraseña de un ordenador. Este ordenador pertenecía al Massachusetts Institut of Technology (MIT) y fue hackeado por uno de sus estudiantes para poder utilizar la sesión de otros compañeros o acceder a la cuenta de un profesor.

El número de ataques hasta este momento no era muy elevado, sin embargo, con la consolidación en la sociedad de los ordenadores personales y el internet, el número de ciberataques aumentó exponencialmente. A finales del siglo XX, las estafas por correo electrónico, conocidas como *phishing*, crecieron sobre manera. Además, los virus informáticos empezaron a propagarse por correo electrónico o en descargas de archivos maliciosos.

La preocupación generada por este aumento de la cibercriminalidad en todo el mundo provocó que el Consejo Europeo buscase una forma para combatir la cibercriminalidad. Por este motivo, el 23 de noviembre de 2001 fue sellado el Convenio sobre la cibercriminalidad por el Consejo de Europa con la participación de Canadá, Japón y China en Budapest. Con el paso de los años, se unieron nuevos participantes a este convenio hasta llegar a 56 firmantes actualmente. Este convenio entró en vigor el 1 de julio de 2004 y tiene como objetivo buscar medios eficaces para enfrentarse a los ciberataques, la armonización del desarrollo de políticas penales comunes en todos los países y la colaboración por parte de todos los países en la lucha por el cibercrimen [4]. En definitiva, se buscaba un convenio en el que todos los países participantes tuvieran un modelo común frente a este tipo de delitos en el que se basaría posteriormente su propia legislación nacional y la colaboración entre los países para enfrentarse a los ciberdelitos.

En el Convenio de Budapest se definieron cuatro diferentes tipos de ciberdelitos [5]:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

2.1 Tipos de ciberataques más comunes

Como se ha visto anteriormente el número de ciberataques crece año tras año. Además, las empresas sufren cada vez nuevos tipos de ataques diferentes, haciendo que la lista de ciber amenazas sea cada vez más grande. A continuación, se explican algunos de los ataques más populares en los últimos tiempos [6]:

- El *phishing* consiste en una estafa a través de correo electrónico para obtener información confidencial de la víctima, en la que el estafador o *phisher* se hace pasar por otra persona o empresa para ganarse su confianza. Si este tipo de estafa se produce por SMS se conoce como *smishing* y si se realiza por teléfono como *vishing*
- El *ransomware* es un tipo de malware con el que el atacante se hace dueño del equipo víctima y cifra toda la información que contiene. De esta manera, si la victima quiere volver a tener acceso a la información, deberá pagar el rescate económico pedido por el atacante para que le envíe la clave con la que descifrarla.
- El Ataque de Denegación de Servicio (DDoS) busca dejar a un servidor inoperativo, enviándole muchas peticiones a la vez hasta llegar a saturarlo. En los últimos tiempos, se está comenzado a utilizar *botnets* para realizar muchas peticiones desde varios equipos de forma simultánea.
- Una inyección SQL se aprovecha de las vulnerabilidades que se encuentran a la hora de validar la información introducida en una página web con el fin de poder obtener las contraseñas o la información que se almacena en la base de datos de dicha página web.

2.2 Cibercriminalidad en España en el 2020

Durante el año 2020, el número de ciberataques ha crecido de forma significativa en parte debido a la crisis sanitaria, ya que esta propició el aumento y la variedad de los ataques. Los ciberdelincuentes centraron sus ataques en ingeniería social intentando engañar a las personas con campañas de phishing y los organismos públicos y a las industrias con diferentes tipos de ataques con *ransomware*.

En la Figura 2 se puede ver los datos de un estudio realizado por La Interpol para averiguar la influencia de la pandemia por COVID-19 en la ciberdelincuencia [7]. Se puede ver que las campañas de phishing aumentaron en un 59%, los ataques por *ransomware* a organismos o empresas aumentaron en un 36% y que la creación de dominios maliciosos relacionados aumentó en un 22%.

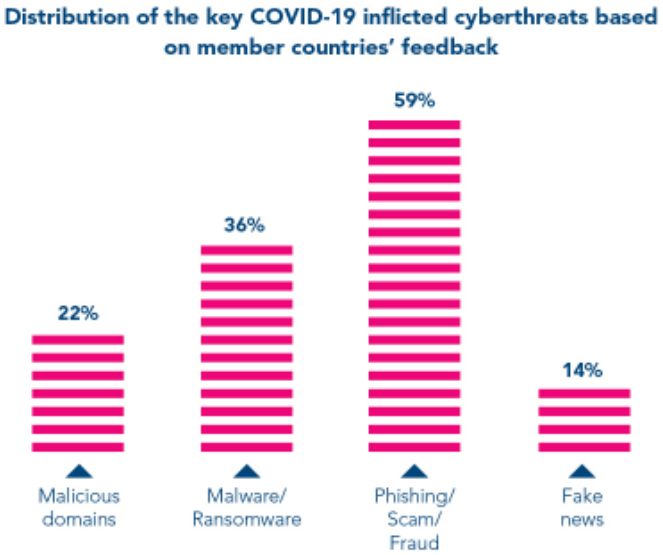


Figura 2: Estudio del aumento de los ciberataques relacionados con el COVID-19 realizado por la Interpol

Según el estudio realizado por el Sistema Estadístico de Cibercriminalidad (SEC) en el año 2020 hubo 287.963 hechos conocidos de ciberataques (Figura 3), aumentando en un 31,9% respecto al año anterior [8] [35]. En esta misma figura, se pude ver que en el año 2021 el aumento no fue tan grande respecto al anterior, siendo del 6,1%. En la Figura 4 se puede ver que solo se ha identificado al autor del ataque el 15% de las veces. Este porcentaje de éxito por parte de las autoridades se ha ido reduciendo año tras año. Esto significa que cada vez los ciberdelincuentes tienen métodos de ataque más sofisticados, logrando que sus ataques tengan mayor porcentaje de éxito y evitando ser detectados por los grupos de ciberseguridad de las autoridades o empresas privadas.

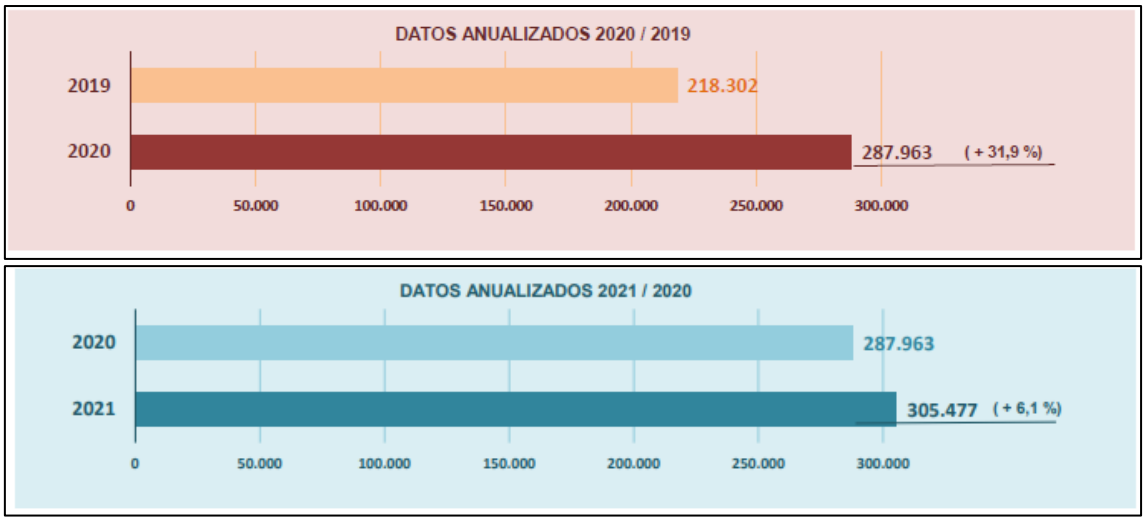


Figura 3: Hechos conocidos en España en los años 2019-2020 y 2020-2021

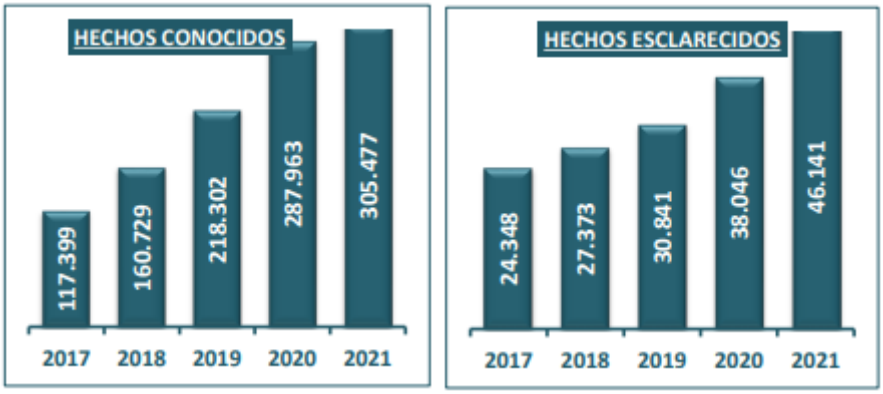
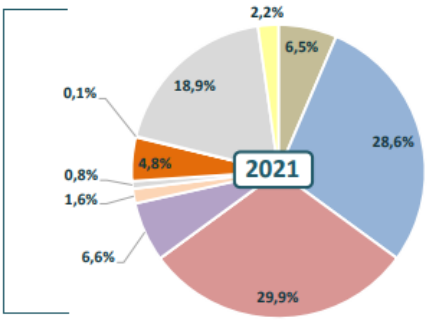


Figura 4: 2021Evolución de los hechos conocidos y esclarecidos en España

En este mismo documento se encuentra un estudio realizado con la colaboración del INCIBE-CERT (Figura 5). El Instituto Nacional de Ciberseguridad en España (INCIBE) se trata de "una entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, red académica y de investigación, profesionales, empresas y especialmente sectores estratégicos" [9]. El INCIBE-CERT es el Centro de Respuesta e Incidentes de Seguridad Informática (CSIRT). En el año 2021 el INCIBER-CERT gestionó 109.126 ciberamenazas [8]. En la Figura 5, se puede ver que los ataques por malware son los más comunes. Uno de los más utilizados y que más daño causa son los *ransomware*. En segundo lugar y a la par de los ataques por malware se encuentran los fraudes, por ejemplo, las campañas de *phishing* y *smishing*.

Tipo de incidente	INCIDENTES GESTIONADOS					
	2016	2017	2018	2019	2020	2021
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039
Fraude	11.843	11.959	55.932	31.938	42.641	31.213
Malware	76.811	81.090	27.016	27.358	46.893	32.605
SPAM	10.279	7.957	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177
Intento de intrusión	381	1.435	396	1.518	1.289	1.753
Robos de información	37	47	63	77	161	920
Contenido Abusivo			9.353	4.064	2.986	5.253
Recolección de información			5.605	84	87	106
Sistema Vulnerable			3.731	31.414	23.161	20.609
Otros	1.038	787	782	4.407	4.409	2.451

Porcentaje del total de incidentes gestionados



*Véase metadatos explicativos

Figura 5: Incidentes gestionados por el INCIBE-CER

Capítulo 3. *El phishing*

El INCIBE define el phishing como la estafa cometida comúnmente a través de correo electrónico, aunque también se puede realizar también por otros medios como por SMS o llamada telefónica, y que tiene como objetivo robar información sensible o las credenciales de acceso de la víctima [6]. Para lograr su objetivo, los atacantes suplantan la identidad de personas u organizaciones de confianza de la víctima.

En los orígenes del phishing, el atacante o *phisher* enviaba el mismo correo electrónico a muchas personas con el fin de que alguna de ellas picara el anzuelo y le entregara sus datos. Por este motivo, el origen de la palabra *phishing* proviene de la palabra inglesa *fishing*, pescar en español, ya que es un buen símil al proceso que realizaba el atacante.

Los *phishers* pueden tener varios objetivos para realizar estas campañas de estafas. Los tres objetivos principales son los siguientes:

- Los datos personales con los que obtienen la dirección de correo, el documento de identidad o los contactos de la víctima, pudiendo suplantar su identidad para poder realizar ataques de *phishing* más creíbles a sus contactos o utilizando los documentos de identidad posteriormente con otros fines.
- La información financiera con la que pueden obtener el número de cuenta o de las tarjetas de crédito o la información sobre el banco de la víctima para robarle el dinero.
- Las credenciales de acceso con las que podrían tener acceso a las redes sociales o el correo electrónico empresarial, entre otros, con los que, al igual que en el primer caso, suplantar la identidad de la víctima para poder alcanzar más víctimas potenciales en entornos a los que antes no podía acceder.

La consultora internacional Deloitte realizó un informe sobre el estado de la ciberseguridad en España en el año 2021 [10]. En él se muestra un análisis exhaustivo realizado a las empresas españolas participantes en el ámbito de la ciberseguridad y lo compara con el año anterior. Según este informe las ciberamenazas más comunes son el *phishing,* el malware y el *ransomware* (Figura 6). Además, una preocupación creciente con relación al *phishing* es el aumento considerable en el *phishing* corporativo o a organismos públicos.

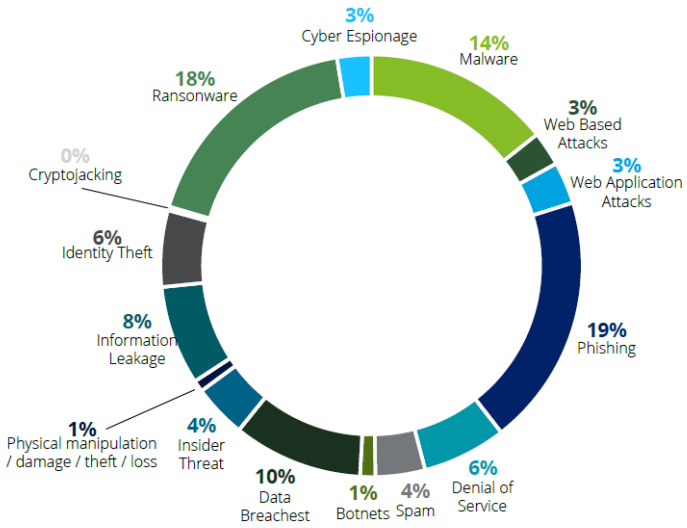


Figura 6: Porcentaje de las ciberamenazas más comunes en el 2021

En la encuesta realizada por la empresa de ciberseguridad Proofpoint se pone de manifiesto la cantidad ingente de ataques de phishing que se realizaron en 2021 [23]. El 91% de los trabajadores afirman que su empresa ha recibido algún tipo de mensaje malicioso de los cuales un 81% tuvo éxito.

3.1 Técnicas utilizadas

El *phishing* aumenta y perfecciona las técnicas que utiliza constantemente con el objetivo de que las víctimas caigan en la estafa. La mayoría de estas técnicas se basan en la ingeniería social para que las víctimas consideren el mensaje recibido como licito y, en verdad, estén siendo engañadas. Las técnicas más utilizadas se explican a continuación.

3.1.1 Uso de subdominios

Esta técnica consiste en utilizar un enlace que contenga un subdominio que imite el dominio de una empresa de confianza, pero el dominio real al que apunta el link es de una plataforma de *phishing* [11]. En la Figura 7 se muestra un ejemplo del uso del subdominio para engañar a la víctima. En este caso se hace creer a la víctima que está accediendo a “Apple” para una oferta de trabajo, cuando en realidad está accediendo al dominio fraudulento “oferta-trabajo”.

Figura 7: Ejemplo de uso de subdominios para engañar a la vícitma

3.1.2 Uso de códigos QR

Debido a la pandemia por COVID-19 el uso de los códigos QR se ha extendido enormemente, ya que sirven para acceder a enlaces a páginas web sin contacto. Entonces, esta técnica consiste en publicar códigos QR maliciosos o modificar los de una entidad legítima, como puede ser el acceso al menú del restaurante o para acceder a la información de un monumento, para que contengan el enlace hacia una página web fraudulenta [12]. El código QR esconde el link y la persona que lo escanea no sabe a dónde le va a redirigir, ya que observando el código a simple vista no se puede deducir si es legítimo o no.

3.1.3 Acortadores de URL

Esta técnica consiste en acortar la URL maliciosa, en cualquier acortador de URLs online, con el fin de camuflar la URL fraudulenta [13]. De esta manera, la víctima desconoce hacía que página web se está redirigiendo. Esta técnica es muy utilizada por correo electrónico, por SMS o en redes sociales. En la Figura 8 se muestra un ejemplo de como la URL "http://www.esto-es-una-prueba-de-phishing.com/" queda totalmente camuflada tras la URL acortada "https://bit.ly/3PTlyMX".

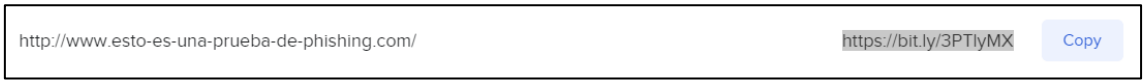


Figura 8: Uso del acortador online, bitly, para acortar una URL maliciosa

3.1.4 Typosquatting

El *typosquatting* consiste en registrar un nuevo dominio fraudulento que se escriba de forma muy similar a uno lícito para que a simple vista parezca el real. Normalmente la diferencia entre el dominio real y el fraudulento consiste en doblar o eliminar alguna letra o sustituir letras muy parecidas por números, por ejemplo, 'l' (ele) por '1' (uno), entre otros casos. En la Figura 9 se muestran varios ejemplos en los que si no se presta atención se puede considera el dominio fraudulento como el verdadero.

Figura 9: Ejemplos de Typosquatting [14]

3.1.5 Ataque homográfico

Xudong Zheng, matemático estadounidense, descubrió en el año 2017 una posible vulnerabilidad con la que se puede enmascarar la URL navegadores que se le dio el nombre de ataque homográfico.

Este ataque consiste en utilizar caracteres Unicode[1] de abecedarios como el cirílico o el ruso, entre otros, que se parezcan a los caracteres del abecedario latino. Entonces, estos caracteres externos al abecedario latino son convertidos por el navegador gracias a Punycode[2] y el usuario no puede distinguir que caracteres son latinos y cuáles no. Por ejemplo, el autor registra en su blog el dominio "xn–pple-43d.com" como si fuera "apple.com" [17]. Lo logra porque la "a" cirílica (U+0430) imita la "a" latina (U+0041).

Este tipo de ataque puede ser más o menos efectivo en función del navegador que utilice la víctima. Se realizó la prueba descrita en su blog, utilizando el dominio "https://www.xn--80ak6aa92e.com/" que imita ser "apple.com" con diferentes navegadores. Usando el navegador Brave te redirige al dominio falso, pero en la URL se ve claramente que es un ataque homográfico (Figura 10). Con el navegador Google Chrome detecta que utiliza caracteres de otros idiomas, te avisa de que la URL podría ser falsa y te da la opción de ir a la página web que trata de imitar este ataque (Figura 11). Sin embargo, Firefox sigue siendo vulnerable a este ataque, ya que te lleva a la página web fraudulenta imitando ser la original (Figura 12).

[1] Unicode: Es un estándar de codificación con el que cada carácter de cada idioma tiene una única codificación [15].

[2] Punycode: Es un estándar de sintaxis de codificación que permite utilizar caracteres internacionales en los nombres de dominio [16].

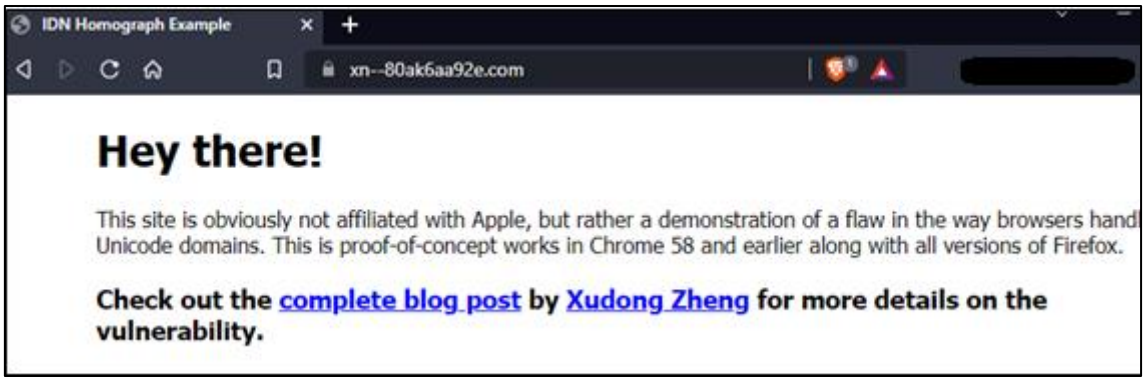


Figura 10:Ataque homográfico en el navegador Brave

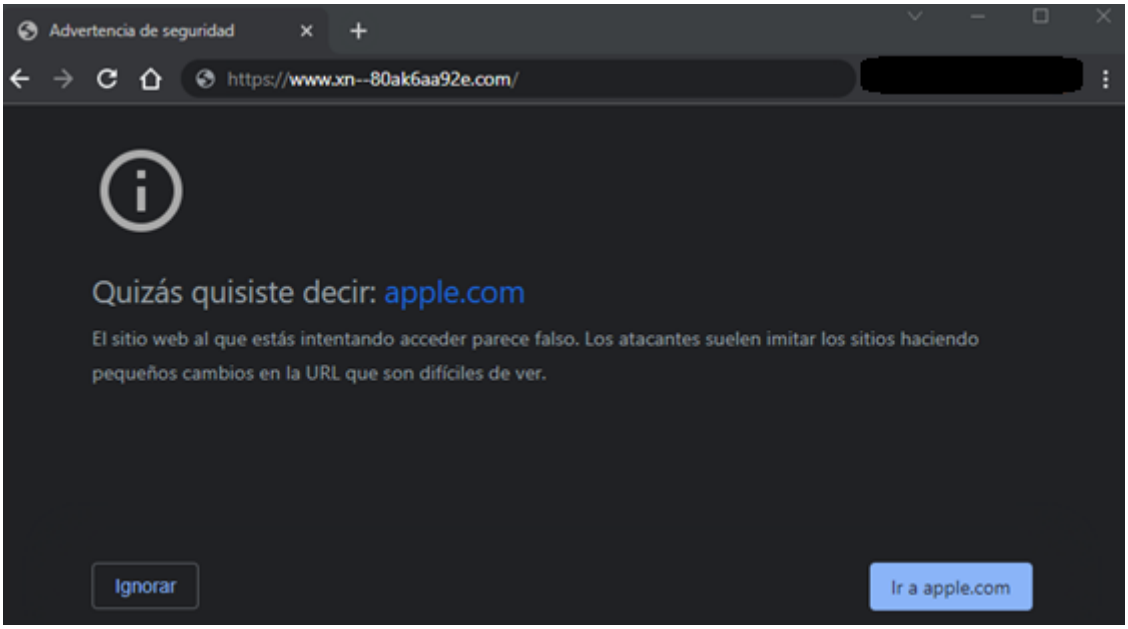


Figura 11: Ataque homográfico en el navegador Google Chrome

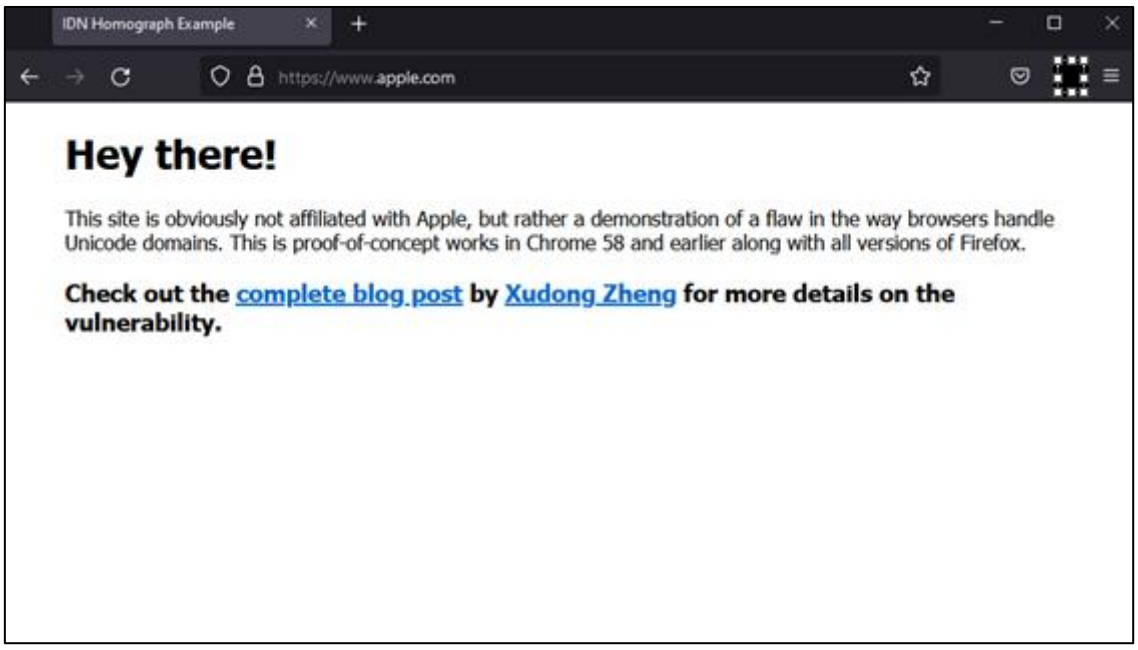


Figura 12: Ataque homográfico en el navegador Mozilla Firefox

3.1.6 Email spoofing

El *spoofing* de correo electrónico se da cuando el *phisher* envía un correo a la víctima haciéndose pasar por otra persona [18]. Para ello, manipula la información del emisor del correo. Esto es posible debido a que el protocolo de correo electrónicos SMTP (Simple Mail Transfer Protocol) no tiene un proceso de autenticación para el emisor del correo lo que permite manipular cierta información del correo electrónico. Además, hay cierta información que no es visible en el correo electrónico que se encuentra en el encabezado, por ejemplo, los timestamps, las direcciones de respuesta o los servidores utilizados para enviar el mensaje.

En la Figura 13 se muestra un ejemplo de *Display Name Spoofing* que consiste en cambiar el nombre del emisor que se muestra en los clientes de correo electrónico por otro de una empresa legítima [19]. En este caso el correo electrónico no ha sido alterado y se puede apreciar que se trata de una dirección de correo que no corresponde con el nombre del emisor. Este ataque es más efectivo en las aplicaciones para móviles, ya que solo muestran el nombre del emisor. Si se quisiera ver la dirección de correo del emisor habría que entrar en los detalles del correo.

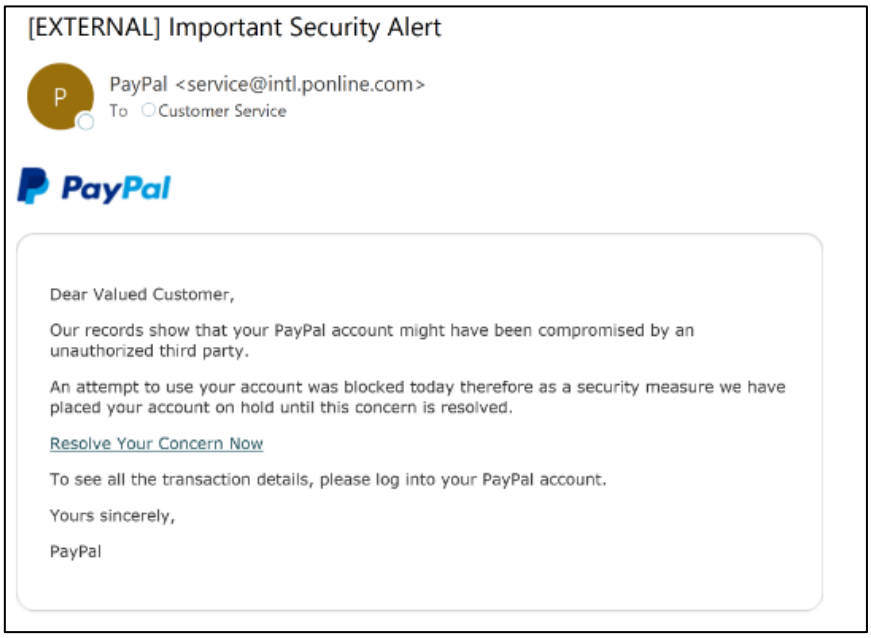


Figura 13: Ejemplo de Display Name Spoofing

Otro tipo de *email spoofing*, el *email addres spoofing* [19]. En el caso anterior solo se modificaba el nombre visible del emisor para parecer un correo legítimo. En este caso, se altera la información de la dirección de correo visible por el receptor para que ésta parezca una dirección real. En caso de combinar los dos tipos, el atacante aumenta considerablemente su porcentaje de éxito, salvo que la posible víctima se fije en los detalles del correo. En la Figura 14 se puede ver que el correo es enviado supuestamente por "bossman@domain1.com", sin embargo, en *reply-*

to se puede ver que quien envió realmente el correo y quien se le respondería sería a el *phiser*, "dude2@domain2.com".

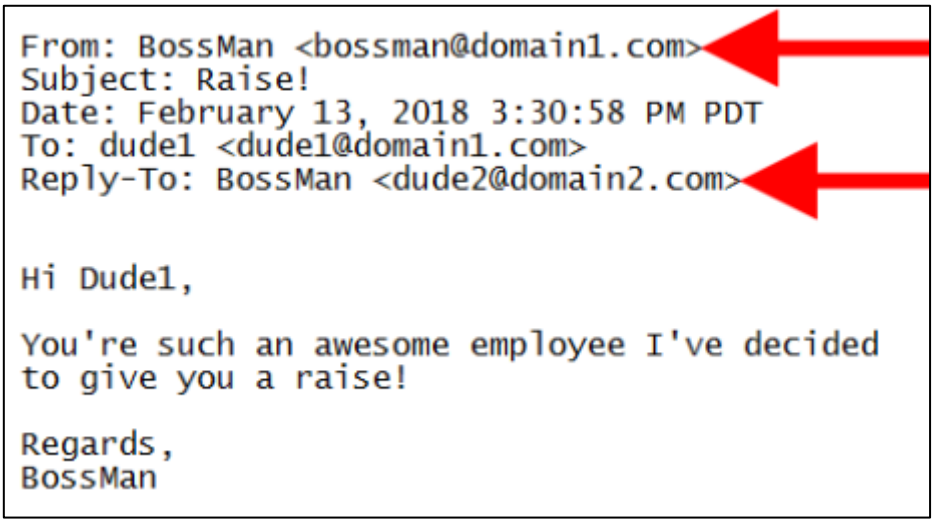


Figura 14: Ejemplo de email address spoofing

3.2 Etapas de un ataque de phishing

Los *phishers* tienen un patrón en la metodología que utilizan para realizar sus ataques. Por tanto, una campaña de *phishing* se puede dividir en cinco etapas [20]. Cada etapa se explica a continuación.

1) Planificación y configuración: Esta primera etapa consiste en definir quién será el objetivo del ataque. Una vez que el objetivo sea definido se procede a obtener información sobre la víctima para que el ataque sea lo más creíble posible. Además, durante esta fase también se elige que tipo de ataque para que este sea lo más efectivo posible en función de la víctima.
2) Ataque: Una vez definida la víctima se procede a enviar el mensaje malicioso a través de un medio telemático, suplantando la identidad de una entidad de confianza de la víctima que se descubrió en la fase anterior.
3) Éxito en el ataque: Esta fase se da cuando la víctima accede a la página web o responde al mensaje malicioso con información sensible o confidencial sobre ella. También se da cuando se descarga el malware adjuntado en el mensaje, si es el caso.
4) Recopilación de información: Una vez que la víctima ha caído en la estafa se procede a verificar y utilizar la información entregada por esta. Dependiendo del tipo de información pedida en el mensaje puede tratarse de los datos bancarios o credenciales de acceso, entre otros ejemplos. Además, si el mensaje malicioso enviaba malware y la víctima lo instalo en su dispositivo, dependiendo del tipo del malware se puede utilizar, por ejemplo, para obtener las contraseñas de sus cuentas o integrar su dispositivo dentro de una *botnet*.

5) Borrar evidencias: Una vez que los atacantes han logrado su objetivo, proceden a eliminar posibles evidencias que puedan utilizar los grupos de ciberseguridad de la policía para identificarlos. Para ello, normalmente se borran los dominios falsos y los servidores y los medios utilizados para realizar el ataque.

3.3 Temáticas de los phishing más comunes

Una de las principales formas de defensa que tiene el usuario es conocer de primera mano cómo son los ataques que más comúnmente van a llegar a su buzón de correo, por lo que siempre deberá estar al día de las campañas de phishing más comunes que existan en cada momento, las cuales, a buen seguro, serán variantes más o menos elaboradas de la siguiente lista de temáticas y formatos:

3.3.1 Cartas nigerianas

Bajo esta denominación se encuentra una de las más antiguas estafas relacionadas con el correo, ya no electrónico, sino ya en el servicio postal tradicional. Ha evolucionado tanto desde sus principios, que se encuentran multitud de variantes, con mayor o menor imaginación. Básicamente consiste en informar al incauto que ha sido agraciado con una herencia, premio o gran cantidad de dinero, procedente bien de un rico africano, familiar (sin problemas, o con problemas requiriendo nuestra ayuda), soldado en algún conflicto armado, o incluso astronautas en la estación espacial. El objetivo puede variar, ya que suele ser para captar "mulas" que realicen movimientos bancarios de dinero "irregular", pero puede dar un giro y pedir dinero, o simplemente, conseguir hacerse con el control de nuestro móvil o de alguna de nuestras cuentas, bancarias o de redes sociales.

3.3.2 Correos electrónicos de entidades financieras

Pocas entidades financieras se escapan a las campañas de phishing que envían los estafadores. Bancos como BBVA, ING Direct, La Caixa, Banco Popular y otros, han sido objetivo de campañas de correos fraudulentos, en los cuales el destinatario es requerido para acceder urgentemente a su banca electrónica a través del formulario que se facilita, el cual, evidentemente, es falso, y solamente permite que el atacante reciba nuestras claves y datos bancarios (Figura 16).

3.3.3 Soporte técnico de empresas y servicios como Outlook, Yahoo!, Apple, Gmail, etc.

Las empresas tecnológicas y de servicios cada cierto tiempo también son objetivo de campañas de correos fraudulentos (Figura 15). De forma parecida al caso de los bancos, y utilizando excusas como: confirmación de la cuenta de usuario, eliminación de cuentas inactivas, detectada actividad sospechosa en la cuenta se ha superado el límite de capacidad de la cuenta, etc, los estafadores tienen como objetivo robar cuentas y datos privados de los usuarios.

3.3.4 Comunicación de alguno de los sistemas de pagos online como PayPal, MasterCard o Visa

Siguen mecanismos similares a los casos anteriores, con variantes como las siguientes: cambio en la normativa del servicio, cierre incorrecto de sesión, mejoras en las medidas de seguridad, cancelación del servicio, etc. Como en el caso de los bancos, los estafadores intentan robar información bancaria y claves de acceso (Figura 13).

3.3.5 Comunicación de la Agencia Tributaria, Tráfico, Ayuntamiento, etc

Al igual que en los casos relacionados con las entidades bancarias, cualquier servicio que incluya movimientos de dinero es susceptible de ser explotado. Las disculpas son más elaboradas: la devolución de dinero a los usuarios, pago de multas o impuestos, etc. Normalmente, se solicitan datos bancarios, o bien se pide dinero que debe pagarse a través de los enlaces incluidos en los correos.

3.3.6 Correos electrónicos de páginas de compra/venta y subastas como Amazon, eBay, etc.

Al igual que en todos los casos anteriores, si hay dinero, hay riesgo. Sin embargo, en este tipo de correos, más originales, se ofrecen falsas tarjetas regalo para comprar en sus tiendas online, lo cual normalmente requiere “fidelizarse”, es decir, dar datos personales y, seguramente, bancarios.

3.3.7 Entregas del servicio de Correos y servicios de mensajería como DHL, FedEx, etc

Bajo el pretexto de “carta certificada no entregada a usted”, o con la excusa de que el paquete enviado no ha podido ser entregado, tienes un paquete esperando, información sobre el seguimiento de un pedido, etc., se pide información personal, o bien se solicita un pago en concepto de aduanas o gastos añadidos.

3.3.8 Falsas ofertas de empleo

Con la excusa de ofrecer un puesto de trabajo, los estafadores primero intentan robar datos privados que pueden ser utilizados posteriormente con distintos fines fraudulentos. Sin embargo, hay también variantes en las cuales de verdad se ofrece “trabajo”, aunque de dudosa moralidad y legalidad, como “mulas”.

3.3.9 Descuentos y “superofertones” de famosas cadenas de supermercados como Lidl, Carefour, Mercadona, etc

Normalmente este tipo de mensajes suelen seguir esquemas de cadenas de mensajes, en las cuales, además de pedirnos datos personales y/o bancarios, ponen como condición para conseguir acceder a las ofertas o sorteos, la “obligación” de “reenviar” el mensaje a un número determinado de contactos, con lo que se perpetúa la estafa.

Capítulo 4. *Tipos de ataques*

Hoy en día el ataque de phishing más generalizado consiste en el envío masivo de correos electrónicos. Anteriormente eran fácilmente detectables porque solían estar mal traducidos, incluir faltas ortográficas o solicitaban información sensible de manera urgente. Sin embargo, en los últimos años están surgiendo nuevos tipos de ataques más sofisticados, más difíciles de detectar, a través de diferentes medios y centradas en víctimas en concreto. A continuación, se explican los tipos de ataques más comunes [6][21][22].

4.1 Deceptive phishing

El deceptive phishing es el tipo de phishing más común de todos y consiste en el envío masivo de correo electrónicos maliciosos, suplantando la identidad de una persona, organismo público o empresa de confianza. En este tipo de ataques no se elige los destinatarios por lo que suele darse el caso que el receptor no tenga ninguna relación con el correo enviado. Además, estos correos suelen ser urgentes o amenazantes, ya que informan de algún error y para solucionarlo se tiene que realizar el proceso lo antes posible. De esta manera, la víctima no presta atención al correo y cae en la estafa.

Estos correos tratan de imitar la apariencia de los correos legítimos y utilizar todas las técnicas mostradas en el capítulo anterior con el objetivo de que la víctima acceda al link y entregue su información. En la Figura 15 se puede ver que el mensaje enviado parece de Apple, sin embargo, si se mira la dirección de envío se puede ver que es una falsa.

El éxito de este tipo de ataque se basa en hacer sospechar a la víctima lo menos posible sobre la falsedad del correo enviado. Por este motivo, para evitar ser estafado, en primer lugar, se debe verificar quien envío el correo y con que cuenta. Además, también es importante verificar si el link que contiene el correo contiene algún acortador o alguna técnica de *typosquatting*. Los navegadores incluyen una función en la parte inferior izquierda que muestra a que página redirige un link poniendo el ratón encima. Por tanto, se debe poner el ratón encima y verificar que la página corresponde con lo que dice ser el correo. También, hay que sospechar cuando un correo te urge a realizar una tarea para recuperar la cuenta o los fondos. Finalmente, como se comentó anteriormente este tipo de correos se envían de forma masiva, por tanto, el correo de la Figura 15 puede ser enviado a personas que no tienen una cuenta de Apple, tratándose claramente de un *phishing*.

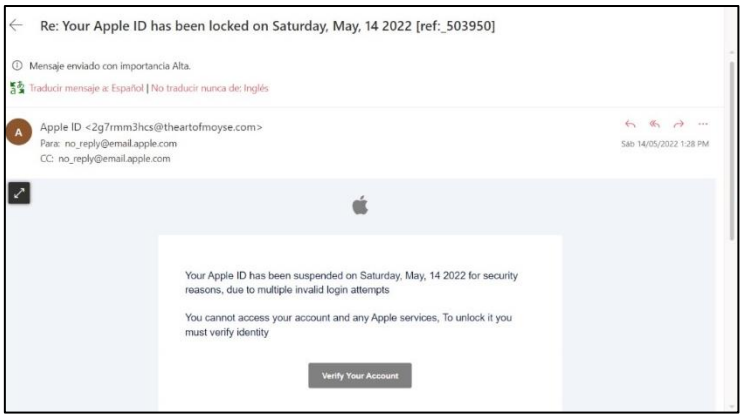


Figura 15: Ejemplo de deceptive phishing

4.2 Spear phishing

El *spear phishing* es muy similar al primer tipo de ataque, sin embargo, realiza el ataque dirigido a una víctima en concreto. Antes de realizar este ataque, el *phisher* ha obtenido información de la víctima para poder realizar un ataque a medida y resulte lo más creíble posible. El objetivo sigue siendo el mismo, lograr que la víctima acceda a la página web maliciosa y entregue su información sensible.

Este tipo de ataque es más difícil de detectar a primera vista porque el atacante se centra en todos los detalles para que el correo parezca legitimo. El *spear phishing* se suele utilizar, robando información la víctima, para acceder a organizaciones.

4.3 Malware-based phishing

Este tipo de ataque utilizan las mismas técnicas, como suplantar la identidad de una entidad de confianza o utilizar *typosquatting*, y el mismo objetivo, robar los datos de la víctima para utilizarlos con fines ilícitos. Sin embargo, el proceso que sigue este ataque es diferente a los anteriores.

Un *malware-based phishing* consiste en enviar un correo electrónico, suplantando la identidad de una persona o entidad de confianza con el objetivo que la víctima descargue el archivo adjuntado en el correo. Este archivo suele tener como nombre algo de interés para la víctima, como una factura o información importante, para que lo descargue e infecte su ordenador.

Los formatos del adjunto malicioso más utilizados son PDF, Microsoft Word o Excel o ZIP. Este adjunto contiene un malware que al ser descargado instala un virus en el dispositivo. Los atacantes suelen proteger los archivos con una contraseña para que el antivirus no lo pueda abrir y detectar si se trata de un archivo malicioso.

4.4 Smishing

No todos los tipos de phishing se realizan por correo electrónico. También, existen ataques que se realizan con el teléfono móvil. Si se realizan por SMS se conoce como *smishing* y se realizan mediante una llamada *vishing,* se verá en el siguiente punto. En el caso del *smishing* se envía un SMS a la víctima normalmente informando de un fallo de seguridad en su cuenta bancaria. Además, al tratarse de un SMS, una URL acortada no hace sospechar a la víctima que, junto a la urgencia del mensaje, accede al link e introduce sus datos para supuestamente arreglar el fallo de su cuenta. En este momento, es cuando cae en la estafa y entrega sus credenciales al atacante.

En la Figura 16 se muestra un ejemplo de *smishing.* En el se puede ver que ha habido un bloqueo y necesita desbloquearlo de manera urgente. Además, en el link se puede ver que supuestamente redirige a BBVA. Sin embargo, utiliza la técnica de los subdominios para confundir a la víctima, ya que el dominio real es "notificaciones-app.ru".

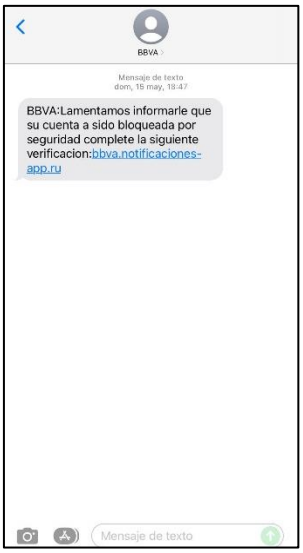


Figura 16: Ejemplo de smishing

4.5 Vishing

Como se comentó en el punto anterior, la otra técnica para estafar a las personas mediante teléfono es el *vishing.* Este tipo de ataque consiste en realizar una llamada a la víctima suplantando la identidad de otra persona. Mediante técnicas de ingeniería social, logra que confíe en él y le entregue sus datos. Normalmente, en este tipo de ataques se ha tenido que realizar un análisis previo de la víctima para que la llamada falsa resulte más creíble.

4.6 Whaling

El *whaling* o el fraude del CEO consiste en suplantar la identidad de un puesto importante en un empresa u organización para engañar a los empleados que controlan los recursos económicos para realizar el pago de una factura falsa o cambiar la cuenta de pago de una nómina por la suya.

Para ello, los atacantes realizan un análisis de la empresa para conocer a sus empleados y los procedimientos utilizados, además, necesitan conocer la dirección de correo electrónico del superior para intentar lograr sus credenciales de acceso o crear alguna similar utilizando el *typosquatting.*

Estos mensajes se caracterizan por ser urgentes y confidenciales. De esta manera se presiona a la víctima para que no pueda verificar si la información es correcta.

4.7 Pharming

Un ataque de *pharming* consiste en aprovechar una vulnerabilidad en el software de los DNS (Domain Name System) para modificar el archivo de resolución de nombres de dominio. De esta manera, el atacante logra redirigir a la víctima a una página web maliciosa, a pesar de que la víctima esté escribiendo correctamente el dominio que quiere visitar.

La página web que visita la víctima es una imitación de la que debería haber sido realmente redirigida. Entonces, en el momento que sea introducido algún dato, estos serán enviados al atacante que decidirá como utilizarlos.

Capítulo 5. *Campañas anti-phishing*

Como se ha visto en el punto anterior, este tipo de estafas han ido evolucionando para hacer más creíbles sus mensajes maliciosos y poder alcanzar a un mayor de víctimas. Además, esto se junta con el desconocimiento de los ciudadanos sobre este tipo de ataques y, si lo son, no son capaces de detectarlos.

En el Capítulo 3 se vio que los ataques por phishing son muy comunes, ya que casi un 90% de las empresas han sufrido al menos uno en el último año. Debido a la alta frecuencia con la que se realizan este tipo de ciberataques, las campañas de concienciación y formación anti-phishing son muy importantes y necesarias. Por ello, es muy importante realizar este tipo de campañas para evitar que el número de víctimas siga aumentando.

5.1 Campañas contra el phishing

Según la encuesta realizada por el INCIBE (Figura 17) solo un 8,4% de los ciudadanos se considera totalmente formado en ámbitos de ciberseguridad [24]. Este desconocimiento es el causante de que los ataques de phishing sean tan exitosos hoy en día como se mostró en el Capítulo 3.

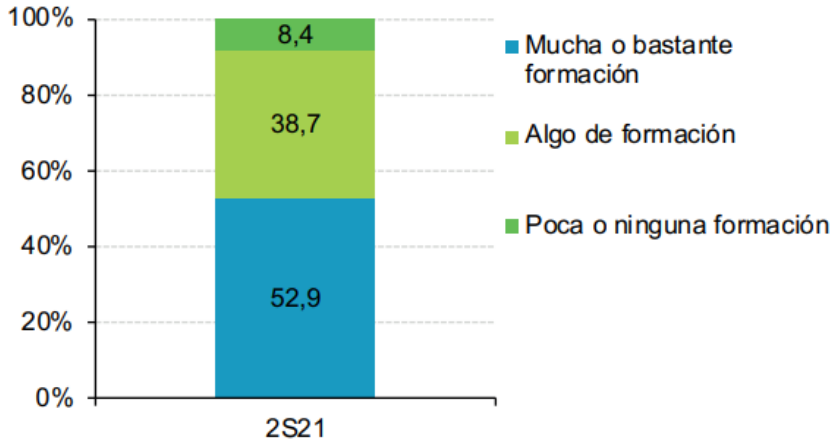


Figura 17: Percepción de necesidad de formación en ciberseguridad (%)

Por ello, la mejor forma de combatir los ataques de phishing, y los ciberataques en general, es educando a la población. Para ello, una buena práctica es informar a las personas sobre los ciberataques, sus tipos y formas de detectarlos (formación) y ponerlas a prueba mediante una campaña de phishing controlada (concienciación). Estas campañas se pueden realizar desde las siguientes instituciones:

- Instituciones gubernamentales: Estas instituciones pueden educar a sus ciudadanos para conocer todos los peligros que se esconde en internet desde los ataques de phishing hasta las *fake news*, ya que la sociedad vive permanentemente conectada a internet y expuesto a sus peligros. Estas campañas pueden realizarse a través de medios digitales, que es el medio por el que existen más campañas, y a través de medios físicos y darlas mayor visibilidad. Realizar estas campañas por medios físicos, por ejemplo, en marquesinas de buses o carteles en los escaparates, es muy importante para llegar a los espectros de la sociedad que no usen tanto las nuevas tecnologías como por ejemplo las personas mayores que, a su vez, son el grupo más vulnerable ante ciberataques.
- Empresas: Las empresas debe considerar realizar campañas de concienciación y simulación de ataque a la empresa, ya que de esta manera sus empleados estarán preparados ante posibles estafas. Además, evitan filtraciones de información sensible, robos de dinero o el ransomware que les perjudicarían gravemente. El ransomware y el phishing suelen combinarse. En España el 71% de las empresas sufrieron un ransomware en el año 2021, por el que un 38% de las empresas pagaron el rescate que de media son 175.344€ [25].
- Centros de enseñanza: Enseñar en los colegios ciberseguridad es muy importante para los nativos digitales, ya que según la Comisión Europea los niños comienzan a navegar por internet más pronto, comenzando desde los 7 años [26]. A esta edad, los niños no son conscientes de los peligros que pueden correr al abrir páginas o descargar aplicaciones maliciosas. Además, comenzar a enseñar a la sociedad sobre estos temas de manera temprana evitará que caiga en futuras estafas.

5.2 Efectividad de las campañas anti-phishing

La realización de campañas anti-phishing es extremadamente importante porque reducen significativamente el porcentaje de éxitos de estos mensajes fraudulentos. La combinación de formar y concienciar a las personas conlleva que las personas ya saben identificar una campaña de phishing y que hacer en dichos casos como se muestran en los tres casos que se van a explicar a continuación.

El primero de ellos se realizó en la Universidad de Toronto (Estados Unidos) [27]. Consistió en realizar los tres tipos de ataques de phishing más comunes de manera: envío de correos electrónicos masivos que pedían que se pinchase en un enlace, se descargase un archivo adjunto o se dieran el usuario y contraseña. Estos ataques se realizaron a toda la comunidad universitaria en enero, abril y julio de 2019.

Los resultados que se obtuvieron fueron muy satisfactorios, ya que se logró reducir en un 64% los ataques de phishing exitosos (Figura 18).

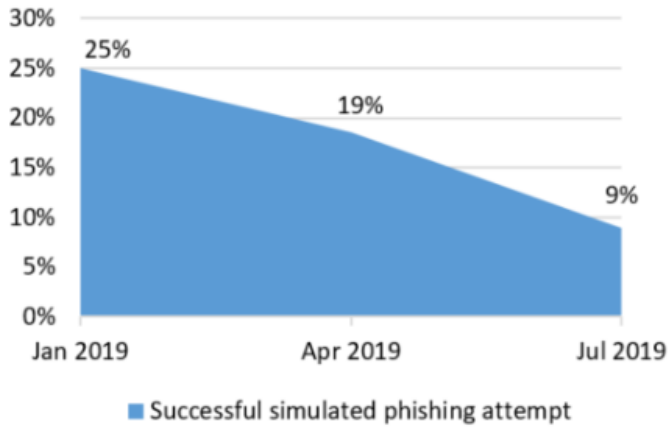


Figura 18: Ataques de phishing exitosos durante la campaña de concienciación

La segunda campaña se trata de un Trabajo Fin de Grado realizado en Argentina a personas con una media de edad de cuarenta años en el 2018 [28].

Esta campaña tenía una duración de quince minutos y constaba de las siguientes partes:

- Primero, se realiza una pequeña introducción a la actividad y una explicación sobre el phishing.
- En la segunda parte trata de una evaluación en la que se muestra al usuario capturas de diferentes páginas web y deberá identificar si se tratan de páginas web maliciosas o no.
- El siguiente paso es realizar una breve encuesta.
- La tercera parte es diferente para las personas que realizaron correctamente la evaluación y las que no. Las personas que no tuvieron ningún error terminan la actividad y a las que tuvieron algún error se les ofrece una formación sobre ciberseguridad. Al finalizar esta formación, se vuelve a realizar una evaluación similar a la de la segunda parte. Tras esta segunda formación se finaliza la actividad.

Esta encuesta arroja un dato muy interesante y es que, a pesar de estar en plena era de la información, el 20% de los encuestados nunca habían oído hablar del phishing. El desconocimiento es la principal causa de la efectividad de las campañas de phishing, por eso, cabe remarcar la importancia de realizar este tipo de campañas.

De todos los participantes un 29% realizó la primera evaluación de manera correcta por lo que no tuvieron que hacer la formación ni la segunda evaluación.

Las personas que no acertaron todas las preguntas tuvieron un porcentaje de acierto del 67% en la primera prueba y, tras realizar la formación, el porcentaje de éxito aumento hasta el 80% lo que supone una mejora en trece puntos gracias a la formación impartida.

También, el autor aporta la mejora que se produjo tras la formación para cada tipo de señal de alerta de phishing (Figura 19). Analizando los resultados se pueden ver grandes mejoras en evitar páginas sin un protocolo seguro (HTTP) o detectando *typosquatting.* Sin embargo, casi no hubo mejoras en el caso en el que phisher utilice subdominios para engañar a su víctima.

Los resultados de esta campaña también muestran una mejora significativa gracias al sistema de formación utilizado. Además, esta campaña es muy útil, ya que también permite identificar que tipos de ataques son más efectivos y hay que dar más importancia durante la formación.

Tipo de error	Mejora global (%)
Páginas web no seguras (HTTP)	54
Typosquatting	45
Uso de subdominios	7

Tabla 1: Mejoras tras la formación según el tipo de error presentado

5.3 Recursos anti-phishing

5.3.1 Recursos ofrecidos por organismos públicos

El INCIBE, que pertenece al Ministerio de Asuntos Económicos y Transformación Digital de España, tiene como objetivo mejorar los conocimientos en ciberseguridad y la confianza digital de los ciudadanos españoles. Para ello, utiliza varias metodologías diferentes para llegar a todos los espectros de la sociedad.

Respecto al phishing cuenta con las siguientes herramientas [9]:

- Campañas de formación. La página web del INCIBE cuenta con un blog en el que explican en que cosiste el phishing y como evitar ser víctima suya. También, muestran carteles en los que resumen todos los pasos a seguir para contrarrestar el phishing que los ciudadanos pueden utilizar o las empresas pueden imprimir y colgar para sus empleados (Figura 19). Por último, informan de todas las nuevas campañas de phishing que están surgiendo para ser conocedores de estas y no caer en ellas.

  Por otra parte, también cuentan con cursos gratuitos sobre ciberseguridad adaptados para empresas y autónomos. En el curso explican todos los riesgos asociados a la tecnología y como utilizarla de manera segura.

  Por último, ofrecen dos metodologías más interactivas que las anteriores y con las que es más fácil llegar a la población más joven. La primera de ellas es un juego de rol en el que se simula un ciberataque. Con este juego se busca mejorar las habilidades frente ataques y gestión de crisis. La segunda metodología consiste en el videojuego “Hackend, se acabó el juego” para todas las plataformas. En este videojuego formarás parte de una empresa

que ha sufrido varios ataques y tendrás que analizar a que se deben los ataques y proteger a la empresa de futuros ataques.

- Kit de concienciación. Se trata de una herramienta didáctica para concienciar y entrenar a los empleados para que usen de manera segura la tecnología y tratar de suplir la falta de preparación de estos. Este kit cuenta con una programación para utilizarlo de forma eficiente, teoría para formar a los empleados y la simulación de dos tipos de ataques: phishing y ficheros maliciosos en USBs infectadas y adjuntos de correos.
- Herramientas. El INCIBE también cuenta con tres herramientas para ayudar a las empresas en la lucha contra los cibercriminales. La primera de ellas se trata de un análisis de riesgos que se realiza en cinco minutos. Consiste en la realización de una prueba para conocer cómo se utiliza la tecnología y las posibles malas prácticas que se pueden dar. La segunda es un documento que incluye todas las políticas de seguridad que ha de seguir una empresa. La última de ellas, es un catálogo de ciberseguridad en el que se encuentran todas las empresas que ofrecen soluciones, productos y servicios en el ámbito de la ciberseguridad.

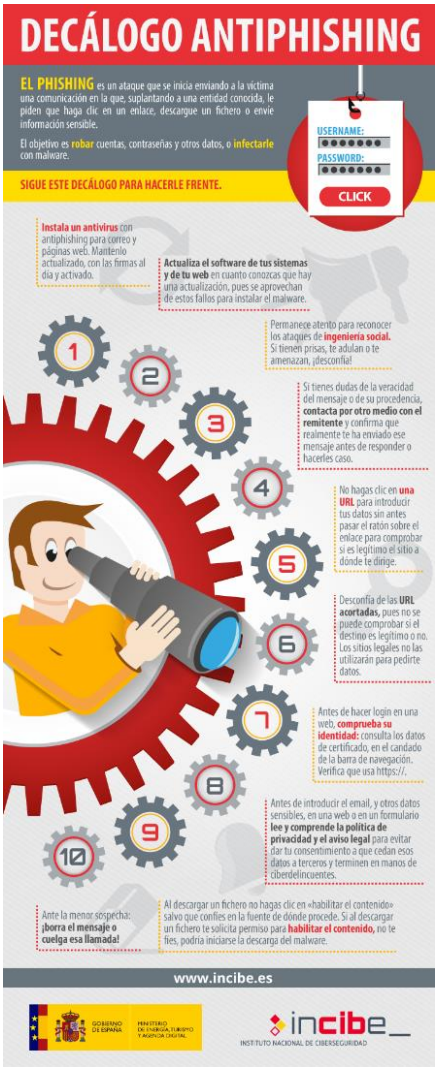


Figura 19: Decálogo antiphishing ofrecido por el INCIBE para empresas y particulares

La Policía Nacional junto a la Universidad de Salamanca sacaron un programa de formación gratuito bajo el nombre "C1b3r Wall Academy" [29]. Es un curso online formado por quince módulos que abarcan la Blockchain, ciberseguridad, Inteligencia Artificial y el Big Data.

Respecto al ámbito de la ciberseguridad, los cursos son impartidos por ponentes experimentados en este campo. Comienzan hablando sobre los fundamentos en ciberseguridad y conciencian sobre todos los posibles ciberataques explicando casos reales. También, explican como tener un entorno seguro tanto personal como laboral. Finalmente, entrando en un nivel más profesional, muestran técnicas de pentesting y análisis forense para detectar posibles vulnerabilidades y saber por dónde entró el cibercriminal al sistema respectivamente.

5.3.2 Recursos ofrecidos por empresas privadas

Las entidades bancarias suelen ser las elegidas por los phishing para ser suplantadas. Por este motivo, muchos bancos cuentan en su página web con información sobre el phishing: que es, como identificarlo y que hacer en caso de ser víctima de este tipo de estafa.

Grandes consultoras en ciberseguridad como ofrecen sus servicios online. Consultoras como Deloitte o Proofpoint ofrecen informes anuales analizando en detalle las ciberamanezas, los problemas que causan y si los usuarios están preparados ante estas situaciones. También, incluyen opiniones y recomendaciones por los expertos en este campo.

Las consultoras en ciberseguridad también ofrecen sus servicios para simular ataques a la empresa para detectar las posibles vulnerabilidades que pueda tener y encontrarle una solución. De esta manera, tanto la infraestructura como los empleados serán más resistentes frente ciberataques.

Por último, también ofrecen servicios en concienciación y formación en seguridad informática especifica y personalizada para proteger la información de las empresas. Estos curos pasan por varias fases: evaluar las posibles vulnerabilidades de la empresa, educar a los empleados, analizar y adaptar la formación a la política de la empresa y reforzar dichos conocimientos.

El Anti-Phishing Working Group (APWG)es un consorcio internacional formado por empresas muy influyentes como Microsoft o McAfee que busca eliminar el phishing y todos los problemas relacionados a este [30]. Este consorcio cuenta con un servicio de formación pública llamado "*APWG Public Education"*. En el cuentan con recursos para la formación y la simulación de campañas.

En el año 2009, realizaron una campaña de concienciación, que se sigue utilizando, para utilizar practicas seguras en el uso de internet y unificar a las empresas y los gobiernos de todo el mundo en la lucha contra el phishing. Esta campaña recibe el nombre "STOP. THINK. CONNECT. Messaging Convention" y está desplegada en dieciocho países, por ejemplo, España, Los Estados Unidos de America y Japón.

Esta campaña global tiene los siguientes recursos: slogan y logo global, videos de formación, carteles para los trabajadores en diferentes idiomas y campañas de simulación de ataques.

5.3.3 Recursos online

En internet es fácil encontrar multitud de recursos para protegerse ante ataques de phishing y aprender a detectarlo y evitarlo. A continuación, se explicarán las herramientas más utilizadas.

Las herramientas anti-phishing más populares son:

- Los antivirus incluyen servicios de seguridad antiphishing normalmente como extensiones en los navegadores. Estos bloquean páginas web maliciosas, muestran opiniones de otros usuarios para saber si la página es confiable o no y pueden bloquear URLs sospechosas que se encuentren en redes sociales. Algunos ejemplos son: Panda Safe Web o Avira Browser Security.
- Hay protectores de correo que mediante una inteligencia artificial analizan los correos recibidos en búsqueda de alguno que sea malicioso. En caso de que alguno haya tenido éxito, estas herramientas también realizan copias de seguridad periódicas para evitar dejar al cliente sin información. Algunos de ellos también cuentan con cursos de formación. Alguna de estas herramientas son Mimecast o Avananan.

Los simuladores de campañas de phishing más usados son:

- Gophish es una plataforma de código abierto disponible para todas las plataformas [31]. Es una herramienta sencilla de instalar y utilizar y permite realizar una campaña de phishing personalizada, ya que se puede definir el emisor del correo y las plantillas del correo y de la página web fraudulenta. Además, también ofrece un panel de control en el que se pueden ver los resultados de la campaña y cuantas personas han mordido el anzuelo.
- Lucy es un producto de ThriveDX y cuenta con una versión de pago y otra gratuita [32]. Con Lucy se pueden realizar campañas de phishing personalizadas como con Gophish, pero además incluye ataques de spear phishing, smishing y con archivos maliciosos. También, incluye cursos de formación para educar a los trabajadores y plugins de correo para detectar posibles phishings.

Capítulo 6. *Elaboración de una herramienta antiphishing*

Como se ha visto hasta ahora, el número de ciberataques han crecido en gran manera, generando muchos problemas a los ciudadanos y las empresas. El objetivo de muchos de estos ataques son los trabajadores, ya que son el eslabón más débil para lograr robar la información a una empresa. Por ello, la formación y la concienciación en este campo es muy importante para evitar fugas de información o dinero. Por estos motivos, con este TFM se busca realizar una herramienta para ayudar en la lucha contra el phishing.

6.1 Objetivo de la herramienta

La herramienta consiste en una aplicación para dispositivos Android empresarial en la que incluye un apartado de formación en ciberseguridad. En este caso, se ha añadido este apartado a una aplicación ficticia de la Universidad de Cantabria, pero este módulo es extraíble y adaptable a cualquier aplicación propia que usen las empresas. Además, también cuenta con una campaña de concienciación contra el phishing en la que se realizará un ataque de phishing controlado a todos los usuarios registrados en la aplicación. De esta forma, los usuarios serán conocedores de los ciberataques más comunes que se realizan contra empresas y sabrán detectarlos en caso de recibir alguno. Con el ataque controlado, serán conscientes de que se pueden recibir ataques de phishing en correos internos y podrán a prueba sus habilidades contra ellos.

Entonces, esta herramienta consta de dos partes:

- Aplicación Android. Se ha desarrollado la app “PhishingUC” que simula una aplicación para estudiantes y profesores de la UC y cuenta con el apartado de ciberseguridad. Este apartado consta de tres partes: un reto de diez preguntas en las que el usuario tendrá que indicar si se trata de un intento de phishing o no, una parte de teoría en el que se explicarán diferentes tipos de ataques y un apartado de estadísticas sobre los ciberataques en España para que darle más visibilidad a lo común que son este tipo de ataques. La aplicación también cuenta con un sistema de acceso y registro de usuarios mediante una base de datos.
- Ataque de phishing controlado con Gophish. Gracias al sistema de registro de usuarios a la app, se obtiene la información necesaria para poder realizar una campaña de phishing. Esta campaña está enfocada a los estudiantes, ya que se utilizan plantillas de correos que simulan la entrega de las calificaciones efectivas. Además, está campaña es mucho más efectiva contra los estudiantes recién ingresados, porque aún no conocen como son los correos enviados y por los nervios y el ansia de conocer las primeras

calificaciones en la universidad no prestan atención a las alertas de una posible estafa.

6.2 Desarrollo de la aplicación

La aplicación se desarrolló para dispositivos Android, porque este sistema operativo cubre la mayoría del mercado de dispositivos móviles y tiene una barrera de entrada menor para los nuevos desarrolladores. Dentro de este sistema operativo existen dos lenguajes que son soportados oficialmente por Google: Kotlin y Java. PhishingUC está desarrollada en Kotlin, ya que es un lenguaje más moderno y sencillo que Java, está perfectamente integrado con Android Studio y Google ya ha mostrado su preferencia sobre Java.

Para la base de datos se eligió Cloud Firestore de Firebase [33]. Esta pertenece a Google por lo que la integración con un proyecto de Android es sencilla. Cloud Firestore es una base de datos NoSQL que permite sincronizar, almacenar y consultar información de una aplicación de manera global.

Una vez indicados los recursos utilizados, a continuación, se explica el funcionamiento de la aplicación.

La aplicación cuenta con sistema de inicio de sesión y de registro de nuevos usuarios, gracias al sistema de autenticación de Firebase. En la pantalla de inicio de sesión se pide al cliente que ingrese su correo electrónico y contraseña para acceder a la app (Figura 20). De no tener estas credenciales, se puede crear un nuevo usuario en el apartado de registro. En este proceso de registro se solicita el nombre, apellido, rol dentro de la universidad, correo electrónico y contraseña. Esta información se guarda en la base de datos y luego se utilizará para realizar un ataque personalizado y controlado de phishing (Figura 21).

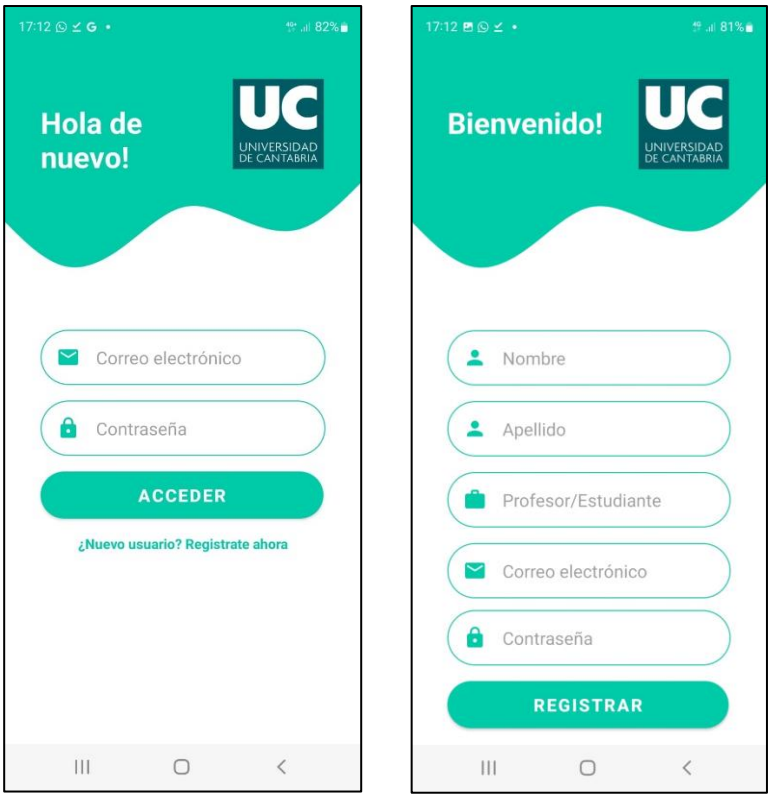


Figura 20: Pantallas de inicio de sesión y registro

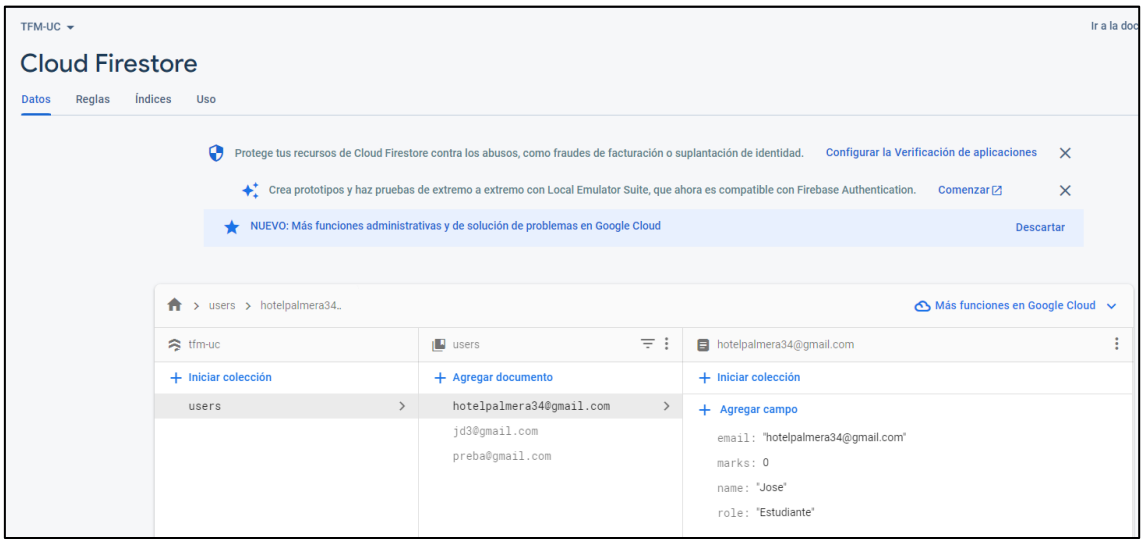


Figura 21: Información de usuario registrada en Cloud Firestore

Una vez iniciada sesión, se muestra el menú principal (Figura 22). En él se han implementado varios botones para que tenga la apariencia de una aplicación real, sin embargo, el único botón operativo es el de ciberseguridad. Además, la aplicación recibe de manera personalizada al usuario, recogiendo su nombre de la base de datos y mostrándolo por pantalla.

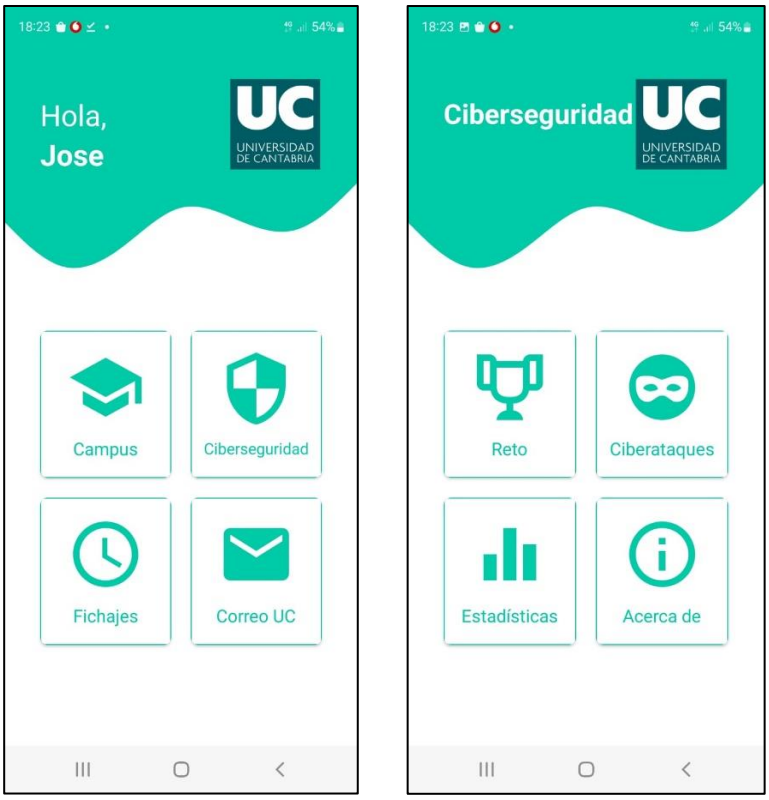


Figura 22: Menú principal y apartado de ciberseguridad

Pinchando en el botón de ciberseguridad, la aplicación muestra los métodos los diferentes métodos que se han implementado para formar a los usuarios. Consisten en un reto de diez preguntas, un apartado de teoría en el que se explican los ataques más comunes, otro apartado de estadísticas para hacer ver que los ciberataques son más comunes de lo que se pueda pensar y, por último, una sección en el que se explica la aplicación y se presenta a la mascota ayudante, Phi, que acompañará al usuario durante su transcurso en la aplicación.

Como se ha comentado, el reto consta de diez preguntas de opción múltiple en la que una solo será la correcta (Figura 23). Todas las preguntas siguen el mismo patrón: se muestra una imagen de un posible intento de estafa y el usuario deberá escoger si se trata de un intento de phishing, fraude del CEO, smishing o es un mensaje legítimo. Tras responder la pregunta, se mostrará la solución y, en caso de ser errónea, se podrá consultar con Phi la solución de la pregunta.

Al terminar el test, se mostrará la puntuación obtenida y un mensaje personalizado en función de esta. Si se pasa la prueba se premiará al estudiante, en caso contrario, se le incita a que se informe más sobre ciberseguridad en esta aplicación o por internet (Figura 24).

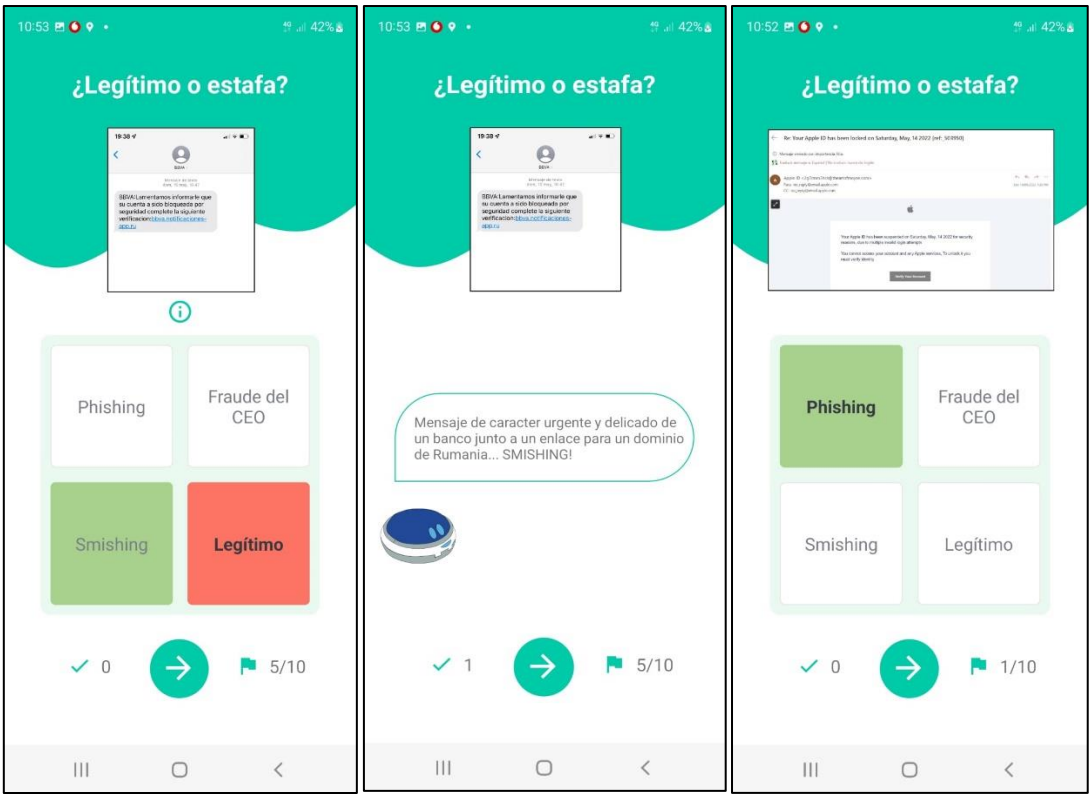


Figura 23: Funcionamiento del test

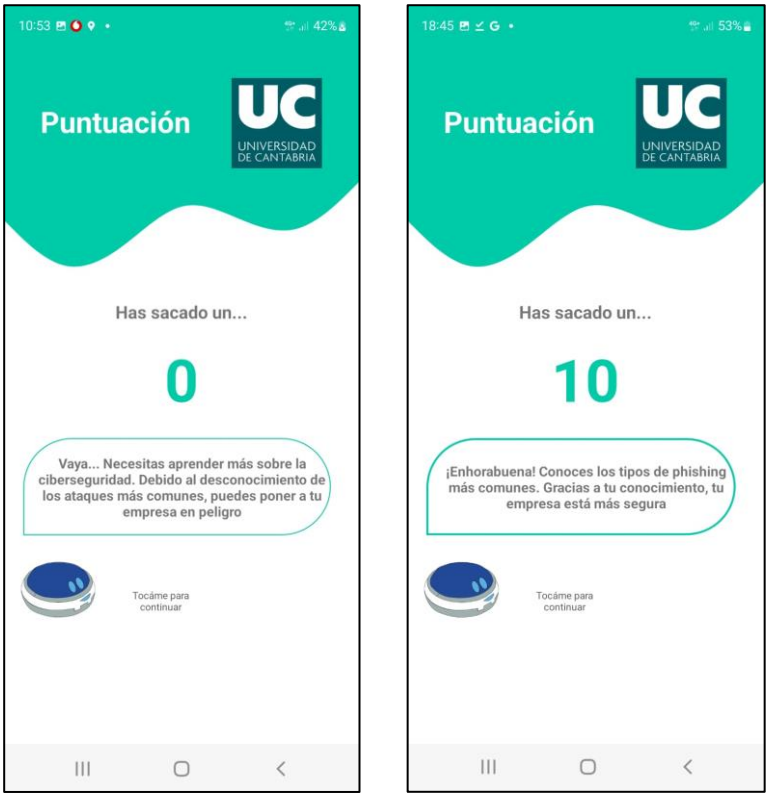


Figura 24: Mensaje personalizado en función de la puntuación

Si el usuario pulsa el botón de ciberataques, le llevará a otra pantalla en el que se le explicará que es y como detectar un posible ataque de phishing, smishing y el fraude del CEO (Figura 25). Estos son los ataques más comunes a empresas por los que se les hace especial atención. También, se explica en menor detalle que es el ransomware y el spear phishing. En la Figura 26 se ve la explicación del phishing para los otros casos la explicación es similar.

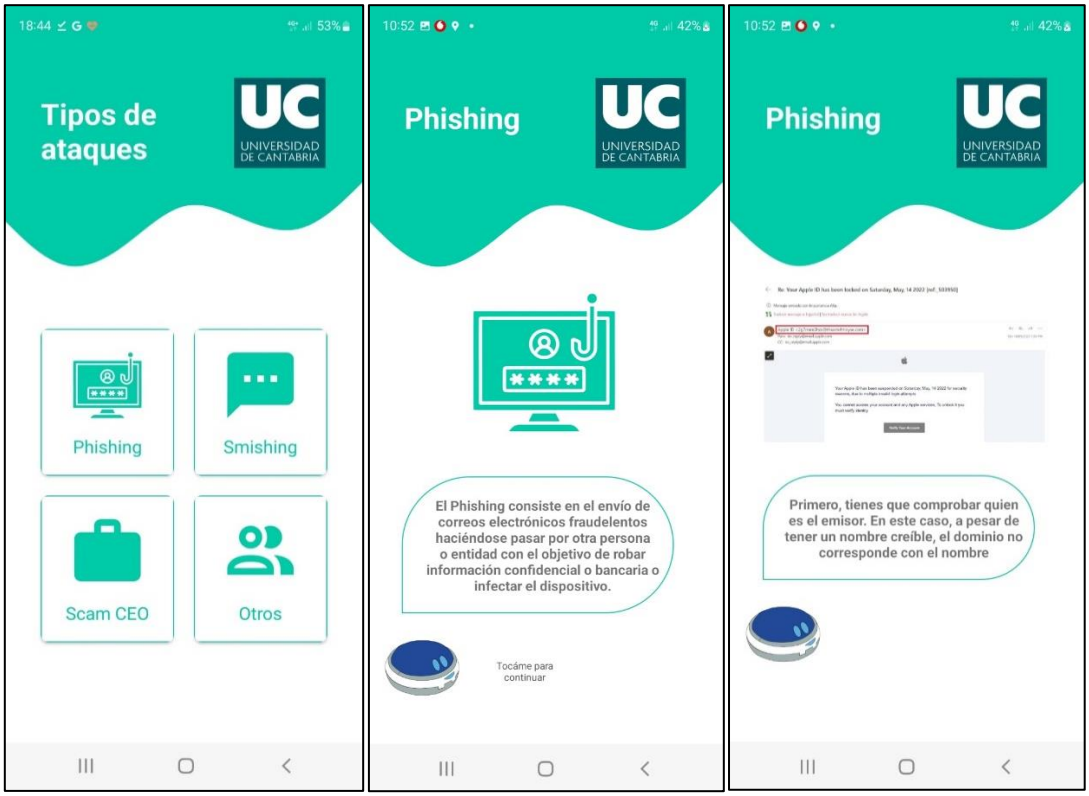


Figura 25: Ejemplos de ciberataques

El último botón relacionado con la ciberseguridad es el de las estadísticas. Aquí se muestran los altos porcentajes de ciberataques para concienciar al usuario de la gran cantidad de ciberataques que se producen al año y los daños económicos que generan. Además, se muestra una estadística que refleja la baja preparación de los ciudadanos españoles en este ámbito.

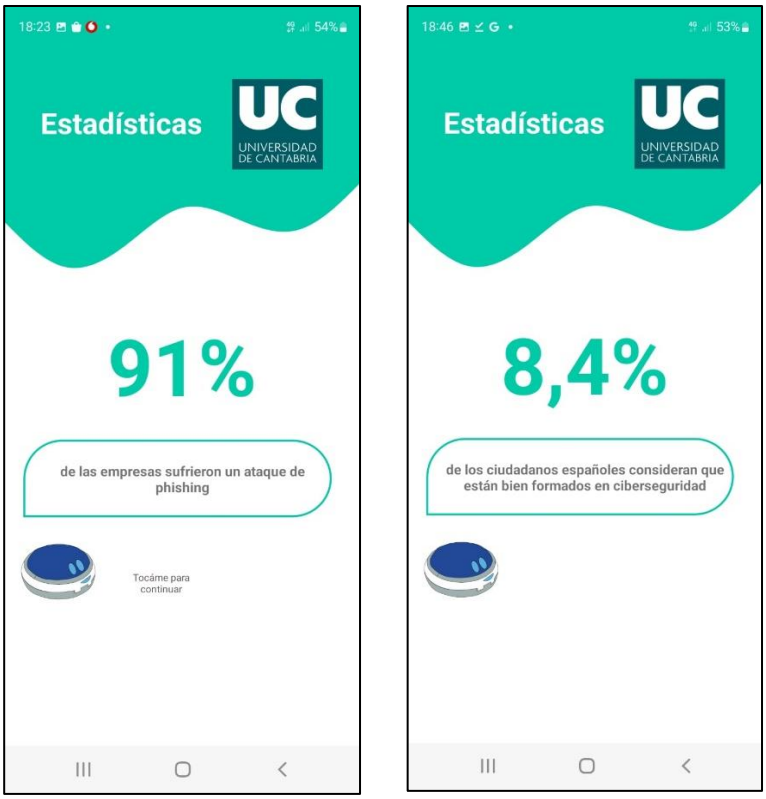


Figura 26: Ejemplos de la sección de estadísticas

Para terminar con la aplicación, se incluyó una sección de información en la que se explicó por qué se realizó la aplicación, los derechos de las imágenes y la presentación del ayudante de la aplicación (Figura 27).

Figura 27: Pantalla Acerca De

6.3 Desarrollo del ataque controlado

Mostrar todos los pasos para configurar la campaña y porque se Eligio gophish

Esta es la segunda parte del desarrollo de la herramienta antiphishing. Consiste en simular un ataque de phishing para entrenar las habilidades de detección de ataques de los estudiantes de la universidad. Para ello, se utilizará Gophish [31].

Se eligió Gophish porque, como se explicó anteriormente, es una herramienta de código abierto, sencilla de configurar y utilizar y totalmente configurable. Además, presenta una consola en la que se muestran las estadísticas de los resultados obtenidos tras la campaña.

La instalación de Gophish es muy sencilla [34]. Primero, se descargan los archivos necesarios desde su página oficial. A continuación, es necesario abrir el fichero "config.json" y configurarlo como sea necesario. En este fichero se definen: la dirección IP y puerto en la que se encuentra el panel de administración y de la página web maliciosa, entre otros parámetros de configuración. Para probar esta herramienta se realizará en local, ya que para alojar la página web maliciosa es necesario pagar un VPS (Virtual Private Server). Tras editar este fichero, se lanza el ejecutable y se accede al panel de control desde el navegador, indicando la dirección IP y puerto escritos en la configuración.

La primera vez que se acceda a la página web requerirá autenticarse con un usuario y una contraseña que se pueden ver tras lanzar el ejecutable. Una vez dentro, ya es posible elaborar, personalizar y lanzar la campaña de phishing.

Primero, se crea el perfil desde el que se enviará el correo de phishing. En el menú principal se accede a *Seding Profiles* y se crea un nuevo perfil. En la Figura 28 se muestran que campos hay que rellenar y como se ha hecho para esta campaña. Como esta campaña se va a realizar en la universidad, se ha creado un perfil de envío haciéndose pasar por ella para que el correo resulte lo más real posible. Por tanto, se utiliza como nombre "Universidad de Cantabria" y se utiliza un nuevo correo de envío creado para esta ocasión "UCantabria@outlook.es" para tratar de confundir a los estudiantes.

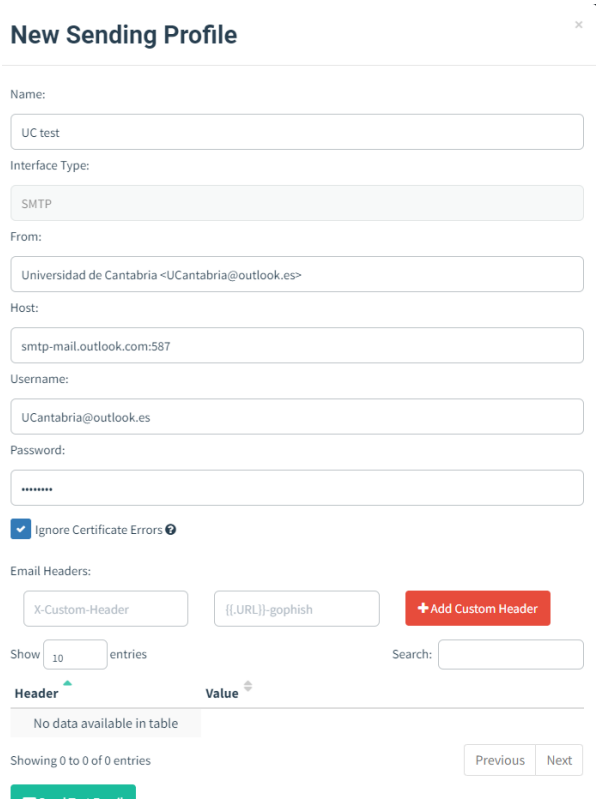


Figura 28: Perfil de envío

Una vez configurada la dirección de envío, se procede a realizar la plantilla para el elemento más importante de la campaña, el mensaje del correo electrónico. Gophish permite utilizar plantillas totalmente personalizables y complejas que pueden engañar a las víctimas con facilidad. Para ello, hay que acceder al apartado *Email Templates*. En este caso se va a simular el correo que es enviado para mostrar las calificaciones definitivas (Figura 29). Se ha tratado de imitar lo más posible un correo legítimo, pero, a su vez, como se trata de un entrenamiento se han añadido características de la mayoría de los correos de phishing: faltas de ortografía, enlace oculto y dotar de urgencia al correo. Además, gracias al registro realizado en la aplicación se puede hacer un correo más personalizado, utilizando el nombre de la víctima como saludo.

Figura 29: Correo oficial enviado por la UC (arriba) y correo enviado por Gophish (abajo)

El siguiente paso es configurar a que página será redirigida la víctima si pincha en el enlace. Se accede a la sección *landing page* y desde aquí se puede programar con HTML. Gophish también ofrece la opción de clonar una página web real. Aprovechando esta funcionalidad y para que vaya en consonancia con el mensaje del correo, se decide clonar la página de acceso al Campus Virtual de la Universidad de Cantabria. En la Figura 30 se puede observar que la página web es idéntica a la real y la única forma de identificarla como maliciosa es observando la URL.

Gophish se puede configurar para que recoja los datos introducidos en la página web y así saber si la víctima se registró en la página web. Sin embargo, no se eligió la opción de guardar las contraseñas introducidas, ya que estas se almacenan sin cifrar en la base de datos de Gophish.

Finalmente, en este apartado también se puede definir a que página será redirigida la víctima si introduce sus datos y le da al botón de "entrar". Normalmente los phisher redirigen a sus víctimas a la página oficial que están suplantando para hacer creer a la víctima que introdujo mal sus credenciales. En este caso y como se trata de una campaña de concienciación se redirigirá a la víctima a la sección de phishing del INCIBE para que sea consciente que ha caído en una "estafa" y pueda aprender para evitar caer en futuras ocasiones (Figura 31).

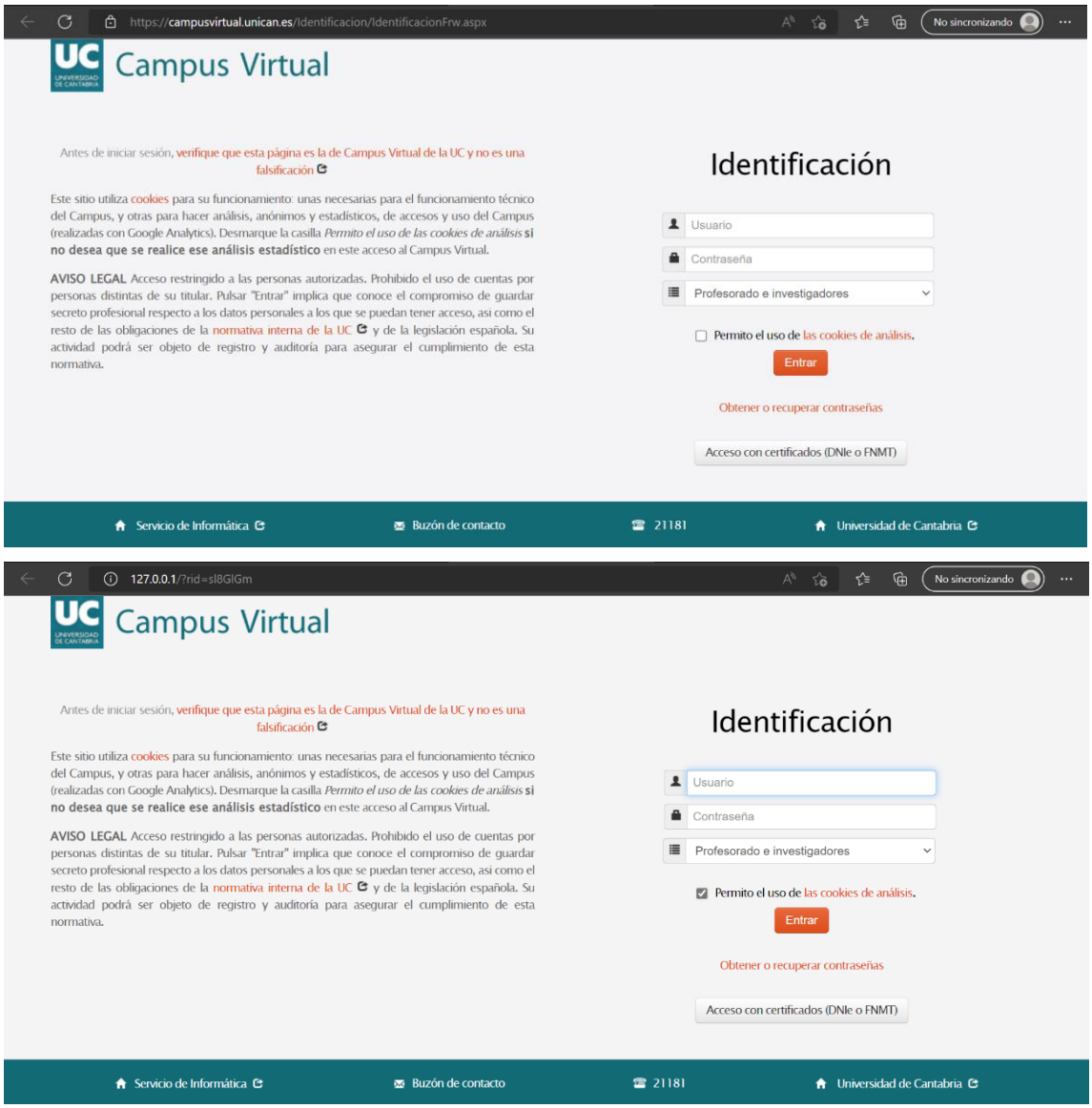


Figura 30: Página real (arriba) y de aterrizaje (abajo)

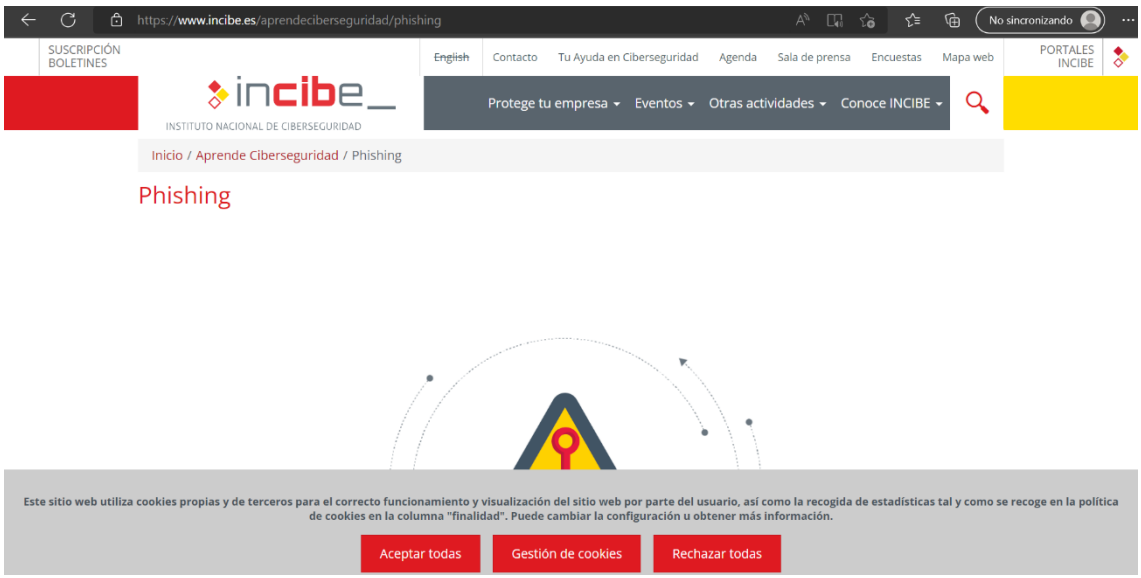


Figura 31: Redirección tras introducir las credenciales

Para terminar con la configuración de la campaña es necesario crear un nuevo grupo desde la seccion *Users & Groups* y programar el envío de la campaña desde la opción *Campaigns*.

En los grupos se define la información de las personas a las que se va a enviar el correo electrónico. Esta información consiste en nombre, apellido, correo y rol dentro de la empresa. Estos datos coinciden con los pedidos en el registro de la aplicación. Además, Gophish ofrece la opción de importar una lista de usuarios mediante un fichero CSV. Esta funcionalidad se complementa bien con Cloud Firestore, ya que con la versión de pago se puede exportar los datos en formato CSV con lo que este paso se podría realizar de forma automática.

En la programación de la campaña se escoge la plantilla de correo y de pagina de aterrizaje, el grupo al que se va a enviar, el perfil de envío y la fecha de envío. El momento óptimo para enviar los correos de phishing es durante el periodo de exámenes de la universidad, ya que es en este momento en el que se envía este tipo de correos. Hacer esta campaña en otras fechas sería muy sospechoso para los estudiantes.

Tras enviar la campaña, se habilita la opción de ver los resultados de esta. En la Figura 32 se puede ver que se muestran las estadísticas sobre correos enviados, correos abiertos, las veces que se ha pinchado el link, las veces que alguien ha introducido sus datos y las veces que el correo ha sido reportado. Además, abajo se puede ver información más detallada sobre la actuación de cada persona contra este correo electrónico.

Figura 32: Resultados de la campaña

6.4 Funcionamiento de la herramienta completa

En los puntos anteriores se ha mostrado el funcionamiento de las dos partes por separado. En este punto se explicará el funcionamiento de ambas partes en conjunto y cuál sería el uso que le daría un estudiante promedio.

Para facilitar la compresión, en la Figura 33 muestra un esquema con la experiencia de usuario durante esta campaña y, a continuación, se explicará cada paso.

Paso 1: Mediante publicidad en la universidad el alumno descubre la aplicación y la descarga en su teléfono inteligente desde Google Play.

Paso 2: El usuario accede a la app y se registra. Este proceso de registro desencadena dos acciones de la que el usuario solo es consciente de una. Por una parte, al registrarse accede al menú principal de la aplicación. Por otra parte, los datos utilizados en el registro son almacenados en una base de datos y luego serán utilizados por un administrador para confeccionar la campaña de phishing. De esta segunda parte, el usuario no es consciente para que así la campaña sea más realista y eficiente al no saber que recibirá un ataque de phishing en un futuro.

Paso 3: El estudiante elige en el menú principal la opción de ciberseguridad. En esta nueva pantalla, puede elegir hacer una prueba para saber sus conocimientos, aprender la teoría sobre los ciberataques o ver algunas estadísticas sobre la efectividad de los ciberataques, que son los pasos 4, 5 y 6 respectivamente.

Paso 4: En esta parte el usuario realiza un reto de diez preguntas en las que se presentan cuatro posibles opciones que solo una es correcta. Si el estudiante se equivoca, tiene la opción de ver la solución. Al terminar la prueba se le mostrará su puntuación y un mensaje personalizado. Si aprueba, se le felicita y anima a que siga aprendiendo más sobre ciberseguridad. Si suspende, se le recuerda la importancia de la ciberseguridad y lo peligrosos que son los ciberataques, además, se le incide en que debe aprender más en ciberseguridad. La puntuación que haya sacado se queda almacenada en la base de datos para que se pueda utilizar en un futuro para, por ejemplo, realizar conclusiones sobre el conocimiento de los alumnos en este ámbito.

Paso 5: En este paso, se le explicará al estudiante el phishing, el smishing y el fraude del CEO sobre un caso práctico de estafa real. Sobre esos mensajes, se le irá mostrando todas las señales de alertas que hay que saber reconocer para no ser víctima de este tipo de ataques. También se le explicará, pero en menor medida, sobre el *spear phishing* y el *ransomware*.

Paso 6: Para terminar con la aplicación, el usuario puede acceder a la sección de estadísticas para ser consciente de la cantidad de ciberataques que se producen y los daños que pueden llegar a causar. Concretamente, se le mostrará el porcentaje de phishing y de éxito de estos en las empresas españolas, el precio medio de un rescate de *ransomware* y el porcentaje de ciudadanos españoles que se consideran bien formados en ciberseguridad.

Paso 7: Desde este paso hasta el paso doce, el usuario de la aplicación no es consciente. Como se dijo anteriormente, es con el objetivo de que esta campaña se lo más efectiva posible. Tras registrarse en la aplicación, su nombre, su apellido, su rol en la universidad y su correo electrónico se quedan almacenados en la base de datos.

Pasos 8 - 11: El administrador recoge los datos de la base de datos y configura la campaña de Gophish personalizada para cada estudiante. También, la programa para que esta se realice durante el periodo de exámenes de la universidad. El día que esté programado, Gophish enviará automáticamente los correos electrónicos a los estudiantes registrados en la aplicación.

Paso 12: El estudiante recibe un nuevo mensaje en su correo electrónico. Él deberá decidir si se trata de un mensaje real de la universidad y acceder al Campus Virtual para ver sus calificaciones, cayendo en la trampa, o reportar el mensaje por estafa.

Paso 13: Se cual se la decisión que haya tomado el estudiante, esta queda guardada en Gophish con la que después se mostrarán los resultados de la campaña. A partir de estos resultados, la universidad puede decidir si realizar campañas de concienciación más intensivas, ofrecer cursos de formación, o la medida que mejor se adapte a estos resultados.

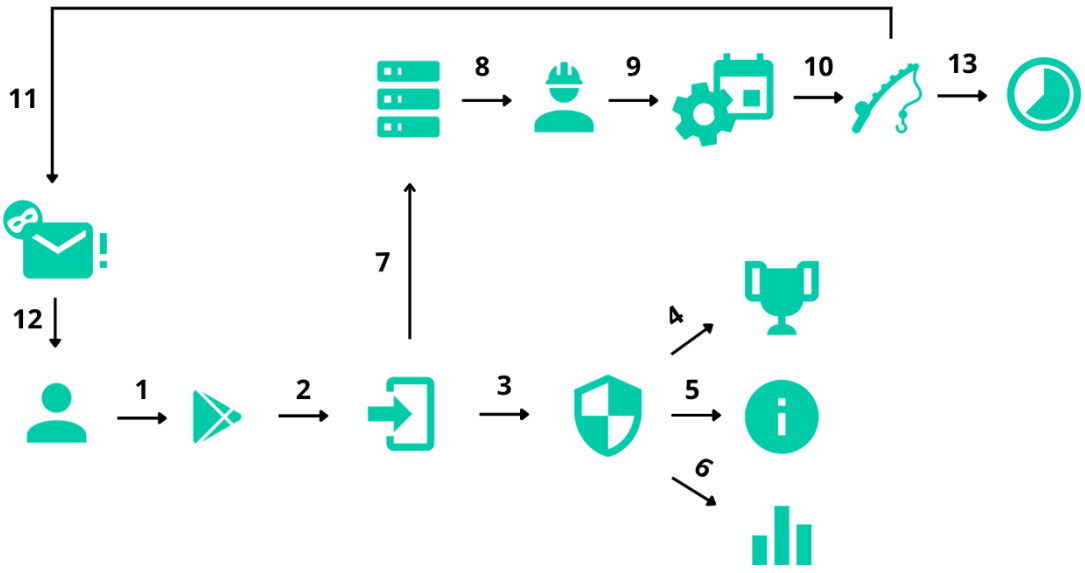


Figura 33: Funcionamiento de la herramienta de antiphishing

Capítulo 7. *Conclusiones y líneas futuras*

7.1 Conclusión

En este Trabajo Fin de Máster se comenzó investigando sobre los ciberataques más comunes. Analizando los estudios y estadísticas citadas en este documento uno se hace consciente de la magnitud de este problema. Según los estudios, prácticamente toda la población ha recibido un ciberataque y la mayoría de estos han sido exitosos. Este alto porcentaje de ciberataques se debe a que la mayoría de los ataques consisten en enviar mensajes de manera masiva, ya que con que un pequeño porcentaje caiga en la estafa a ellos ya les sale rentable.

Otro dato preocupante obtenido de los estudios es la baja preparación de los ciudadanos españoles en ciberseguridad. Solo un porcentaje muy bajo se consideraban preparados y capaces de detectar un ciberataque y reportarlo. Este bajo porcentaje se puede deber a que muchas personas no son conscientes de los peligros que entrañan internet, son personas novatas en este mundo o son ciudadanos que no terminan de adaptarse a las nuevas tecnologías, por ejemplo, las personas mayoras.

A lo largo de este TFM se han ido explicado varios tipos de ciberataques, pero el tema principal es el phishing. Sobre este se ha explicado que es, los tipos que existen y las técnicas más comunes utilizadas por los phishers. Estas técnicas se centran en la ingeniería social y en conocimientos algo avanzados en informática que la mayoría de las personas no conocen. Este también puede ser un motivo del porcentaje de éxito que tiene el phishing.

Por estos motivos, se llegó a la conclusión que el gran porcentaje de éxito de los ciberataques se deben en gran medida al desconocimiento de los ciudadanos. Los estudios sobre las mejoras en la detección de ciberataques son muy satisfactorios, ya que gracias a estas campañas se logra reducir el éxito las estafas por internet de manera notable. Por lo tanto, es muy importante que se comience a invertir en la formación de las personas para que estén preparadas ante estas situaciones.

A raíz de la conclusión anterior, se llega a otra conclusión. Se ha visto que la formación de los ciudadanos es muy importante, sin embargo, desde el gobierno se realizan pocas campañas que tengan una gran visibilidad para personas que no pasan mucho tiempo en internet o desconocen el término del phishing, ya que toda la información que el INCIBE u otros organismos ofrecen se encuentran de manera online y hay que ir a buscarla de manera propia. Por ello, se deberían realizar campañas anti-phishing que lleguen a todos los espectros de la sociedad, por ejemplo, en la televisión, las marquesinas de los buses o carteles colgados en lugares públicos. Además, las empresas también deberían realizar este tipo de campañas para proteger su información, ya que hay un porcentaje alto que aún no forman a sus trabajadores en este ámbito.

7.2 Líneas futuras

La campaña de concienciación realizada se puede ampliar de varias maneras.

- La parte de simulación de un ataque de phishing se puede realizar para todos los empleados de la universidad. También, se pueden utilizar otras herramientas para simular otros tipos de ciberataques como smishing, uso de malware o vishing. Además de solo enviar un correo de phishing anual, se pueden enviar varios correos de forma aleatoria al año y de diferentes índoles.
- La aplicación para Android se puede ampliar añadiendo información sobre otros ciberataques, nuevos tipos de preguntas en el reto que sean más interactivas o con nuevas secciones. Estas nuevas secciones pueden ser: recomendación de creadores de contenido divulgadores sobre ciberseguridad, un minijuego relacionado con este ámbito o un blog con post sobre ciberseguridad.

Aparte de las ampliaciones en las partes elaboradas en este Trabajo Fin de Máster, también se pueden contactar con empresas privadas o públicas para que impartan cursos de manera presencial u online y realizar jornadas de puertas abiertas en la que se realicen charlas de expertos en el sector.

Bibliografía

[1] We are social, “Digital 2020: EL uso de las redes sociales abarca casi la mitad de la población mundial” [En Línea]. Disponible: https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital/

[2] UNODC, “La ciberdelincuencia en resumen” [En Línea]. Disponible: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html#:~:text=La%20ciberdelincuencia%20es%20un%20acto,%2C%202012%3B%20Maras%2C%202014%3B

[3] Xiaomei Han, “Trastorno en el mundo inalámbrico, breve historia de cibercriminalidad y los casos cibercriminales durante las pandemias sanitarias del siglo XX”, Revista crítica de historia de las relaciones labrales y del apolítica social, pp. 21-36, 2020

[4] Nuria Fernanda Cordero Ruiz, “La ciberdelincuencia”, Trabajo Fin de Máster, Universidad de Alcalá, 2021

[5] Council of Europe, “Convenio sobre la ciberdelincuencia”, Serie de Tratados Europeos nº 185, Hungría, 2001

[6] INCIBE, “Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario”, 2021

[7] Interpol. “Un informe de la Interpol muestra un aumento alarmante de los ciberataques durante la epidemia del COVID-19” [En Línea]. Disponible: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

[8] Javier López Gutiérrez, Francisco Sánchez Jiménez, David Herrera Sánchez, Francisco Martínez Moreno, Marcos Rubio García, Victoria Gil Pérez, Ana María Santiago Orozco, Miguel Ángel Gómez Martin, “Estudio sobre la criminalidad en España”, Dirección General de Coordinación y estudios, 2020

[9] INCIBE, “INCIBE” [En Línea]. Disponible: https://www.incibe.es/

[10] Deloitte, “El estado de la cibersguridad en España”, Deloitte Cyber Strategy, 2022

[11] Alain Messina Valverde, “Diseño e implementación de una extensión Chrome para la detección de sitios web de phishing utilizando aprendizaje automático”, Trabajo Fin de Grado, Universidad Autónoma de Madrid, 2021

[12] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Cranor "QRishing: The susceptibility of smartphone users to QR code phishing attacks", Camegie Mellon University, Estados Unidos, 2012

[13] Sidharth Chhabra, Anupama Aggarwal, Fabricio Benevenuto, Ponnurangam Kumaraguru, "Phi.sh/$oCiaL, The Phishing Landscape through Short URLs", Delli College of Engineering, 2011

[14] DNSFilter, "Typosquatting: How Hackers are taking advantage of your typos", [En Línea] Disponible: https://www.dnsfilter.com/blog/what-is-typosquatting

[15] Unicode, "Basic Info" [En Línea] Disponible: https://home.unicode.org/basic-info/overview/

[16] A. Costello, "RFC 3492 – Punycode: A bootstring encoding of Unicode for Intern", University of California, 2003

[17] Xudong Zheng, "Phishing with Unicode Domains", [En Línea] Disponible: https://www.xudongz.com/blog/2017/idn-phishing/

[18] Surbhi Gupta, Abhishek Singhal, Akanksha Kapoor, "A literature survey on social engineering attacks: phishing attack", Amity University Uttar Pradesh, India, 2016

[19] NJCCIC, "Spotting a Spoofing" [En Línea] Disponible: https://www.cyber.nj.gov/informational-report/spotting-a-spoofing

[20] Eduardo Benavides, Walter Fuertes, Sandra Sanchez "caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura", Cienc Tecn UTEQ, vol 13, pp 97-104, 2020

[21] Jaime López Sánchez, "Métodos y técnicas de detección temprana de casos de phishing", Trabajo Fin de Máster, Universidad Abierta de Cataluña, 2019

[22] Tripwire, "6 common phshing attacks and how to protect against them", [En Línea] Disponible: https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

[23] Proofpoint, "2022 State of the Phish", 2022

[24] INCIBE, "Como se protege a la ciudadanía ante los ciberrriesgos", Observaciber, 2022

[25] Sophos, "The State of Rasomware 2022", 2022

[26] Garmendia, M., Jiménez, E., Karrera, I., Larrañaga, N., Casado,M.A., Martínez, G. y Garitaonandia, C. "Actividades, Mediación, Oportunidades y Riesgos online de los menores en la era de la convergencia mediática". Editado por el Instituto Nacional de Ciberseguridad (INCIBE), 2022

[27] Universiad de Toronto, “UTM Anti-Phishing Campaign Results”, [En Línea] Disponible: https://www.utm.utoronto.ca/iits/news/utm-anti-phishing-campaign-results-we-re-improving

[28] Patricia Prandini Diego Pascaner, “Efectividad de campañas anti-phishing”, Trabajo Final de Especialización, Universidad de Buenos Aires, 2018

[29] C1b3rWall, “C1b3r Wall Academy” [En Línea] Disponible: https://c1b3rwallacademy.usal.es/

[30] APWG, “APWG | Unifying The Global Respone To Cybercrime” [En Línea] Disponible: https://apwg.org/

[31] Gophish, “Open-Source Phishing Framework” [En Línea] Disponible: https://getgophish.com/

[32] ThriveDX, “Lucy” [En Línea] Disponible: https://lucysecurity.com/es/

[33] Firebase, “Cloud Firestore | Almacena y sincroniza los datos de tu app” [En Línea] Disponible: https://firebase.google.com/products/firestore?hl=es-419

[34] INCIBE, “Manual de implementación de la herramienta Gophish”, Instituto Nacional de Ciberseguridad, 2020

[35] Javier López Gutiérrez, Francisco Sánchez Jiménez, David Herrera Sánchez, Francisco Martínez Moreno, Marcos Rubio García, Victoria Gil Pérez, Ana María Santiago Orozco, Miguel Ángel Gómez Martin, “Estudio sobre la criminalidad en España”, Dirección General de Coordinación y estudios, 2021