

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
- 7. Antiphishing**
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



Antiphishing

7.1. GoPhish - capacitación y concienciación

En esta primer capítulo sobre Antiphishing del ciclo "Aprendiendo Ciberseguridad paso a paso", exploramos cómo utilizar la herramienta "**GoPhish**" para simular ataques de phishing y fortalecer la concienciación en ciberseguridad dentro de las organizaciones.



¿Qué aprenderás en este capítulo?

- Conceptos clave de ingeniería social: Comprende cómo los ciberdelincuentes manipulan a las personas para obtener información confidencial.
- Tipos de phishing: Identifica las diferencias entre phishing tradicional, spear phishing, whaling y vishing.
- Características de los ataques de phishing: Reconoce señales como urgencia, enlaces sospechosos y suplantación de identidad.

- Uso de GoPhish: Aprende a configurar campañas de phishing simuladas para educar y evaluar la preparación de tu equipo.

Basado en el artículo:

"Capacitación y concienciación anti-phishing"

disponible en <https://darfe.es>

Capacitación y concienciación anti-phishing

Alejandro Cornejo Estrada
acornejo@darfe.es



Objetivo del ciclo:

Proporcionar herramientas prácticas y conocimientos teóricos para que profesionales y organizaciones puedan protegerse eficazmente contra las amenazas de phishing.

Ingeniería social

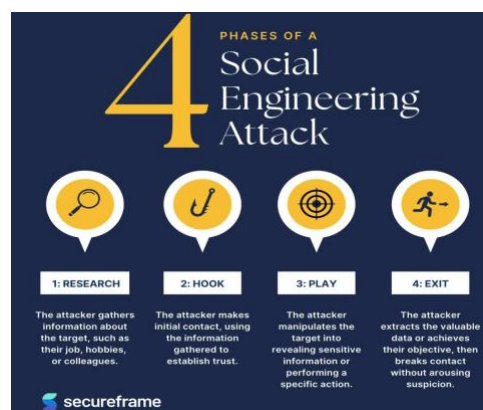
La ingeniería social, en el contexto de ciberseguridad, son técnicas de manipulación utilizadas por ciberdelincuentes para obtener información confidencial, acceso a sistemas, o inducir a una persona a realizar acciones que pongan en riesgo su seguridad. Se basa en la psicología y el comportamiento humano, más que en conocimientos técnicos.

Según Secureframe

(<https://secureframe.com/es-es/blog/social-engineering-statistics>)

Los ingenieros sociales están utilizando tácticas cada vez más personalizadas para ganar confianza y evitar sospechas. La clonación de voz y la tecnología deepfake hacen posible que los actores de amenazas se hagan pasar por sus objetivos de maneras aún más convincentes. En un caso de alto perfil, la voz creada por IA de un director de banco se utilizó para engañar a un gerente de banco y transferir 35 millones de dólares a los actores de amenazas.

Los ataques de ingeniería social son una amenaza especialmente peligrosa para las organizaciones precisamente por el elemento humano. Los errores cometidos por usuarios legítimos son más difíciles de detectar, predecir y remediar. En muchos casos, las víctimas ni siquiera se dan cuenta de que han sido engañadas.



Phishing

El **phishing** es uno de los ataques de ingeniería social más comunes.

El atacante usa correo electrónico, mensajes en redes sociales, mensajería instantánea o mensajes de texto para engañar a la víctima de forma que revele información confidencial, descargue y abra un archivo o visite una web fraudulenta.

Normalmente tienen las siguientes características:

- Tratan de atraer la atención o generar curiosidad. Por ejemplo: *"Acceso indebido identificado en su cuenta bancaria, si no ha sido usted, utilice el link de abajo para asegurarla"*.
- Sensación de urgencia. Esto trata de reducir la posibilidad de que el atacado se dé cuenta de que "algo raro ocurre".
- Uso de **URLs** (Uniform Resource Locator) recortadas (ocultan la URL real) o enlaces incrustados (redirecciones a páginas webs ocultas en parte del texto o imágenes). Esto trata de evitar que los usuarios puedan ver que la dirección a la que van a acceder no es la verdadera o que tiene un nombre sospechoso.

- Suelen tener un asunto engañoso para tratar de emular que el mensaje viene de un origen fiable.
- Copia de logos, textos o imágenes corporativas de la fuente.

Para desarrollar con más detalle el tema, veamos el siguiente video (**Obligatorio**).

 **Anti-Phishing con GoPhish, capacitación y concienciación**
Charla 151 - Aprendiendo Ciberseguridad

<https://youtu.be/i--S0Hj8RF4>



Múltiples recursos afirman que el **90%** de todos los ciberataques comienzan con phishing

Las estadísticas muestran que entre el 80 y el 95% de los ciberataques se inician a través de correos electrónicos de phishing.

- El último informe de CISCO sobre tendencias de amenazas a la ciberseguridad revela que un abrumador **90% de las violaciones de datos** se producen debido a intentos de phishing con éxito.
- El **Informe sobre Amenazas de Phishing de Cloudflare** predice que esta tendencia continuará, ya que el phishing basado en el correo electrónico representará casi el 90% de todos los ciberataques en 2023.
- En línea con estas conclusiones, Comcast Business destaca que aproximadamente **entre el 80% y el 95% de las ciberamenazas** se originan en ataques exitosos que utilizan el phishing por correo electrónico.



7.2. GoPhish - primeros pasos

En esta segundo Tema de nuestra sección de "anti-phishing" del ciclo "Aprendiendo Ciberseguridad paso a paso", nos adentramos en la instalación y configuración inicial de GoPhish en un entorno Kali Linux. Este proceso es fundamental para simular campañas de phishing y fortalecer la concienciación en ciberseguridad dentro de las organizaciones.

¿Qué aprenderás en este tema?

- Instalación de GoPhish en Kali Linux: Descarga, descompresión y ejecución del binario de GoPhish.
- Configuración del archivo config.json: Ajuste de parámetros clave como admin_server.listen_url y phish_server.listen_url para habilitar el acceso remoto y definir los puertos de escucha.
- Consideraciones de seguridad: Recomendaciones sobre el uso de TLS, gestión de certificados SSL y protección del archivo config.json mediante permisos adecuados.

- Acceso al panel de administración: Cómo iniciar GoPhish y acceder al panel de administración a través del navegador.

Basado en la documentación oficial de GoPhish:

Guía de instalación:

<https://docs.getgophish.com/user-guide/installation>

Configuración del config.json:

<https://docs.getgophish.com/user-guide/installation#understanding-the-configjson>

Para desarrollar con más detalle el tema, veamos el siguiente video **(Obligatorio)**.

-  **Anti-Phishing con GoPhish, primeros pasos - Charla 152**
- Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/JgY7wGBIRgY>



7.3. GoPhish – ajustes de configuración

En este tercer tema de nuestra serie "Aprendiendo Ciberseguridad paso a paso", exploramos cómo realizar los ajustes de configuración más importantes para que GoPhish funcione correctamente en entornos corporativos. Este tema es clave para lograr una simulación profesional de campañas de phishing.

¿Qué aprenderás en este video?

- Cómo editar el archivo config.json para permitir el acceso remoto al panel de administración de GoPhish, incluyendo la elección de puertos, direcciones IP, y consideraciones de seguridad.
- Creación de un perfil de envío (Sending Profile): aprende a configurar GoPhish para enviar correos simulados a través de servidores SMTP reales o locales.
- Ajustes de seguridad recomendados: control de accesos, activación de TLS, y configuración segura de las interfaces de administración y phishing.
- Pruebas de envío para validar que tu servidor y perfil están correctamente configurados.

Este video te dará una base técnica sólida para empezar a lanzar campañas educativas reales de concienciación sobre phishing en tu organización.

Dentro de phishing, podemos diferenciar dos tipos que son más peligrosos aún:

- **Spear Phishing o Phishing dirigido**: mucho más peligroso que el phishing normal. Este tipo de phishing requiere más esfuerzo de los atacantes. Su principal diferencia con el phishing normal

es que los atacantes estudian antes contra que víctimas van a realizar el ataque, de forma que el e-mail o mensaje de texto que mandan puede estar dirigido usando datos personales o reales de las víctimas. Esto hace que las víctimas lo consideren con una probabilidad mucho más alta mensajes legítimos y caigan ante ellos, también haciendo que sea más difícil detectarlo como spam. Hoy en día con la IA (como veremos más abajo), este tema es aún mucho más peligroso.

- **Whaling:** son un Spear Phishing dirigido a directivos o individuos con información crítica (de ahí el nombre, ataque de ballenero). Utilizan las técnicas de Spear Phishing, pero normalmente se camuflan como correos de negocio crítico y urgente.

IMPORTANTE: Antes de hacer click en cualquier enlace, comprueba su legitimidad examinando detenidamente la URL. Pasa el ratón por la parte superior de la URL. Si esta dirección difiere de la que se muestra, no hagas click en ella.

Entrando en más categorías de phishing, podemos mencionar también:

- **Vishing:** El vishing es una combinación de las palabras voz y phishing. Se refiere a estafas de phishing que se hacen por teléfono. Se intenta engañar para que se revele información crucial de carácter financiero o personal. El vishing funciona igual que el phishing, pero se lleva a cabo mediante tecnología de voz. Muchos los atacantes utilizan sistemas de IVR (Respuesta de Voz Interactiva) para simular que son centros de atención al usuario o ayuda al usuario y piden a la víctima que llame a un número gratuito, otras veces directamente llaman ellos simulando un agente.

Normalmente tienen las siguientes características:

- Uso de información correcta. Usan métodos informados para obtener información del atacado para dar legitimidad a su engaño.
 - Urgencia.
 - Spoofing telefónico
 - Simulación de Service Desk: la llamada trata de simular muchas veces un centro de servicio al usuario legítimo y podemos escuchar al fondo y ruido de call center, obviamente no es real sino un efecto de sonido incorporado a la llamada.
- **Smishing:** El Smishing es un ataque similar al Phishing o Vishing salvo que utiliza mensajes **SMS** para tratar de engañar a la víctima. Comparte la mayoría de características del phishing.



- **Scams de Voz** (Scam: estafa, timo): Llamadas telefónicas con objeto de estafar o sonsacar datos a la víctima haciéndose pasar por representantes de organizaciones legítimas. Se podría considerar un tipo de phishing, pero la verdad es que los voice scams existen desde antes de la creación del concepto de phishing moderno.

Características típicas:

- Suplantación de organizaciones bancarias, de seguros, salud o estatales.
- Uso de guiones profesionales.
- Urgencia.



el 40% cae en la falsa urgencia de los correos electrónicos de RRHH, saltándose una verificación crucial

La seguridad del correo electrónico es una prioridad absoluta para todo tipo de empresas, ya que los piratas informáticos se aprovechan de nuestro comportamiento rutinario y de nuestra urgencia. El último análisis de KnowBe4 muestra que el 40% de estos mensajes engañosos dirigidos a la manipulación imitan a mensajeros de RR.HH. con el objetivo de tratar a los empleados en términos de estabilidad laboral o falta de tiempo.

Para desarrollar con más detalle el tema, veamos el siguiente video (**Obligatorio**).

 **Anti-Phishing con GoPhish, ajustes de configuración - Charla 153 - Aprendiendo Ciberseguridad**

<https://youtu.be/1XemUIHdKxY>



7.4. GoPhish - Landing page

En esta cuarta entrega del ciclo “Aprendiendo Ciberseguridad paso a paso”, aprenderás a crear una **Landing Page** personalizada con GoPhish. Esta página imita un entorno de inicio de sesión legítimo con fines educativos, permitiendo evaluar la respuesta de los usuarios ante un intento de phishing simulado.

¿Qué aprenderás en este video?

- Cómo clonar páginas reales de login (Outlook, Google, Intranet, etc.) de forma segura y ética para fines de capacitación.
- Cómo construir tu propia Landing Page desde cero en GoPhish.
- Activar la captura de credenciales (simulada, sin almacenar datos reales sensibles).
- Redirección a página de retroalimentación o concienciación después de completar el formulario.
- Buenas prácticas para evitar malentendidos y asegurar la legalidad del ejercicio.

Contenido técnico destacado:

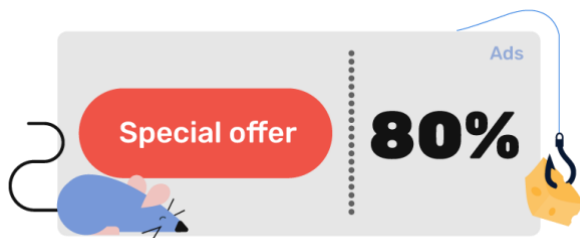
- Uso del editor HTML de GoPhish.
- Inserción del formulario falso.
- Configuración del campo “Capture Submitted Data”.

- Redirección a feedback.html alojado en tu servidor local o de formación.

Este tema marca el momento en que tu campaña de concienciación empieza a cobrar forma práctica. La Landing Page es el primer punto de contacto con el usuario y debe equilibrar realismo con ética profesional.

Siguendo con nuestro artículo, veamos ahora.

- **Baiting o Uso de Cebo** (Bait: cebo)



Las técnicas de Baiting se basan en ofrecer un premio a la víctima, o que consiga algo. Esto puede estar representado como colgar en la web una falsa aplicación para descarga con software malicioso o que el atacante deje tiradas unidades de USB con malware, el objetivo es

que algún incauto los recoja y lo conecte a su computador, infectándolo en el proceso. Durante la pandemia, se puso de moda también los códigos GR falsos, con enlaces a páginas fraudulentas.

Desgraciadamente los ataques de Baiting son bastante efectivos, dado que los seres humanos suelen bajar la guardia cuando están alegres al tener la sensación a haber logrado algo o conseguido un activo gratuito.

- **Scareware** (Scare: asustar)

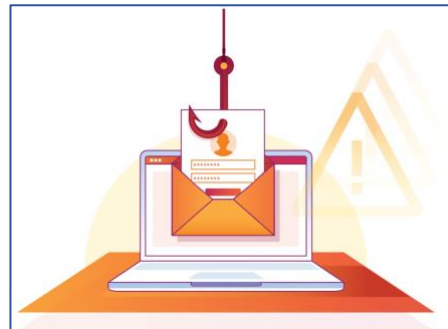
El Scareware es un tipo de ataque y un tipo de software. El Scareware se caracteriza por intentar asustar a la víctima con falsos mensajes de amenaza, urgencia o virus para que llame a un número, mande un correo o realice una acción. La forma de que conseguir que la víctima reciba estos mensajes es normalmente comprar direcciones de web similares a sitios legítimos, de forma que la gente que se equivoca al escribir la dirección legítima acaba en ellos e inmediatamente son bombardeados por pop-ups o banners que tratan de simular mensajes de sistema.



Otras veces el scareware es software que normalmente simula ser un antivirus o antimalware, cuya única característica es mostrar siempre que nuestro sistema tiene muchos errores o riesgo, pidiéndonos que llamemos a un número para asistencia o compremos una licencia. Otras veces el scareware es directamente en sí mismo un virus informático.

Según el **Informe de Cloudflare sobre las amenazas de phishing en 2023**

A nivel global, se estima que el 90% de los ciberataques exitosos comienzan con el phishing por correo electrónico. El impacto financiero medio de una violación de datos causada por phishing se disparó hasta los 4,76 millones de dólares en 2024. Además, el **83%** de las organizaciones fueron víctimas de ataques de phishing exitosos, y el **54%** de estos ataques resultaron en la violación de datos de los clientes.



The Cloudflare BlogMetaComplianceGeekfla (https://blog.cloudflare.com/es-es/2023-phishing-report/?utm_source=chatgpt.com/)

Factor humano: El DBIR 2022 de **Verizon** revela una verdad aleccionadora: el 82% de las violaciones de datos implican la manipulación humana a través del phishing o el robo de credenciales.

La creciente sofisticación de los ataques de phishing, impulsada por el uso de inteligencia artificial (IA) y técnicas de ingeniería social, ha hecho que las campañas sean más personalizadas y difíciles de detectar. Los ciberdelincuentes utilizan herramientas de IA para crear correos electrónicos fraudulentos altamente personalizados, lo que aumenta la probabilidad de éxito de sus ataques.

Financial Times

Ante este panorama, es fundamental que las organizaciones implementen programas de concienciación y capacitación en anti-phishing.



Herramientas de código abierto como **GoPhish** permiten simular ataques de phishing para educar a los empleados y fortalecer la postura de seguridad de la empresa. Estas simulaciones ayudan a identificar vulnerabilidades humanas y a desarrollar estrategias efectivas para mitigar los riesgos asociados al phishing.

Para desarrollar con más detalle el tema, veamos el siguiente video **(Obligatorio)**.

 **Anti-Phishing con GoPhish, Landing page - Charla 154 - Aprendiendo Ciberseguridad**

https://youtu.be/AW9_SEHykHA



7.5. GoPhish - email Template

En esta charla te enseñamos cómo diseñar plantillas de correo electrónico para campañas de phishing simuladas usando GoPhish, una de las herramientas más potentes para entrenar a usuarios y prevenir ciberataques reales.

¿Qué aprenderás?

- Cómo crear un email template atractivo y realista
- Qué elementos incluir para aumentar la efectividad de la simulación

- Buenas prácticas para campañas éticas de concienciación

Un tema muy importante que se presenta en este punto es la configuración de “variables” de Gophish, las cuáles nos permiten (como cualquier otra idea de variable en programación) adoptar cualquier valor preconfigurado.

Las variables más comunes que se suelen emplear son:

¿Qué variables tenemos?	
Variable	Descripción
{{.FirstName}}	Nombre del destinatario
{{.LastName}}	Apellido del destinatario
{{.Position}}	Cargo del destinatario
{{.Email}}	Dirección de correo del destinatario
{{.From}}	Dirección del falso remitente
{{.URL}}	La URL de la página utilizada para simular

Durante el desarrollo del video 155, también se presenta la siguiente teoría:

Importancia de la IA en los ataques de phishing

Estadísticas y tendencias clave en 2025

- **Aumento de quejas por ciberataques impulsados por IA:** Se estima que en 2025 se registrarán aproximadamente 1,31 millones de quejas relacionadas con ciberataques potenciados por IA, con pérdidas potenciales que podrían alcanzar los 18.600 millones de dólares. [ESED](#)
- **Incremento global de intentos de phishing:** Según un informe de Kaspersky, los intentos de phishing han aumentado un 617% a nivel global desde 2022, impulsados por el uso de IA para generar mensajes más creíbles y dirigidos a usuarios específicos. [ITware Latam](#)
- **Eficacia de correos electrónicos generados por IA:** Un estudio académico reveló que los correos electrónicos de phishing generados completamente por IA alcanzaron una tasa de clics del 54%, comparable a los creados por expertos humanos y significativamente superior al 12% de correos genéricos. [arXiv](#)
- **Fraude financiero y deepfakes:** Más del 50% del fraude financiero en 2025 involucra el uso de IA y deepfakes, lo que ha llevado a que el 90% de las instituciones financieras adopten soluciones basadas en IA para detectar y prevenir estos delitos. [Feedzai](#)

Técnicas emergentes potenciadas por IA

- **Spear phishing automatizado:** La IA permite a los atacantes recopilar información específica sobre sus víctimas y generar mensajes personalizados que imitan el estilo de comunicación de personas de confianza, aumentando la probabilidad de éxito de los ataques. [Whalemate](#)
- **Suplantación de identidad con deepfakes:** Los ciberdelincuentes utilizan IA para crear videos y audios falsos que imitan a ejecutivos o empleados, facilitando fraudes como el compromiso del correo electrónico empresarial (BEC).
- **Evasión de filtros de seguridad:** Los modelos de lenguaje avanzados permiten generar correos de phishing que evaden los filtros tradicionales de spam

Para desarrollar con más detalle el tema, veamos el siguiente video **(Obligatorio)**.

 **Anti-Phishing con GoPhish, email Template - Charla 155 -**
Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/Gf7whmiS7Ko>



7.6. GoPhish - New Campaign

¡Pasamos a la acción! En esta charla configuramos desde cero una campaña completa de phishing simulado con GoPhish, enseñándote cada paso para que tú también puedas implementarla en tu organización.

¿Qué verás en este video?

- Cómo crear y lanzar una nueva campaña en GoPhish
- Asignación de targets, landing pages y plantillas
- Seguimiento de resultados y métricas clave

💡 La **concienciación** es la mejor defensa contra el phishing. Este sexto tema, forma parte de una serie práctica para aprender ciberseguridad aplicándola a casos reales.

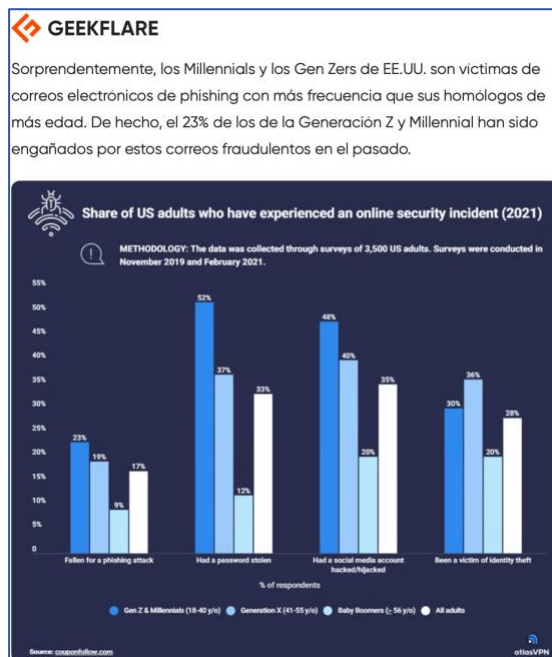
Nuevamente, basados en nuestro artículo, presentamos la parte final del mismo.

Importancia de la Capacitación y concienciación anti-phishing

Como hemos visto, este creciente e imparable volumen de ataques de phishing, potenciando su credibilidad por medio de IA, está generando campañas más personalizadas y difíciles de detectar.

Es importante tener en cuenta que este tipo de ataques, contrariamente a lo que se piensa, tiene mayor impacto en gente joven que en adultos mayores, tal cual lo demuestra otro de los análisis realizado por Geekflare, que presentamos a la derecha.

Esta imagen, nos presenta una nueva visión de esta realidad, en la cual si prestamos atención, podemos ver que en cada una de las gráficas, los mayores porcentajes lo tienen las dos columnas de la izquierda que se corresponden a las edades de: 18-40 años y 41-55 respectivamente, es decir la masa de la base activa empresarial.



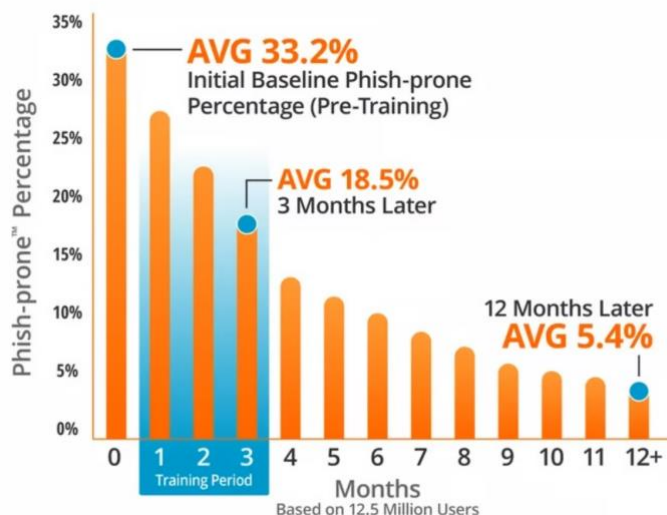
Todos los estudios demuestran que la mejor forma de combatir este tipos de ataques, que reiteramos va en crecimiento exponencial y son el **90%** de los ciberataques exitosos comienzan con el **phishing** por correo electrónico, es por medio de la: **“Concienciación y capacitación”**

Volviendo a los análisis de Geekflare, otra de sus estadísticas, nos pone de manifiesto que los resultados de formación pueden llegar a reducir los efectos de este tipo de ataque a un 5,4% luego de 12 meses de un plan de formación adecuado. Lo podemos ver en detalle en la imagen de la derecha.

Por todas las razones expuestas, es que este artículo, lo hemos pensado como la base teórica de una serie de videos sobre **“Capacitación y concienciación”**, empleando la herramienta Open-Source: **Gophish**.



Las cifras del informe **KnowBe4 2023 Phishing** by Industry Benchmarking Report ponen de relieve los resultados de la formación en materia de concienciación sobre seguridad para los empleados. Según el informe, antes de la formación, cerca del 33,2% de los empleados no eran capaces de superar una prueba de phishing. Esto se ha reducido al 18,5% tras un periodo de 90 días de formación y de nuevo al 5,4% tras un año de formación.



En nuestro **Canal Youtube**, bajo el ciclo **“Aprendiendo Ciberseguridad paso a paso”**

Para desarrollar con más detalle el tema, veamos el siguiente video **(Obligatorio)**.

Anti-Phishing con GoPhish, New Campaign - Charla 156 - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/ILBZZ3euxSY>



7.7. GoPhish - Campaign 2

En este nuevo tema del ciclo sobre GoPhish exploramos cómo planificar y ejecutar una segunda campaña de phishing controlado. Analizamos en detalle cómo optimizar lo aprendido en la campaña anterior.

Ideal para profesionales de ciberseguridad, responsables de concienciación y equipos de TI que quieren reforzar su estrategia de defensa activa.

Aprenderás:

- Cómo duplicar y ajustar campañas anteriores
- Cómo aplicar diferentes Templates (Plantillas)
- Como se presentan las diferentes interacciones de los destinatarios de los mails ante diferentes respuestas
- Evaluación del impacto y mejoras incrementales

¡No te pierdas esta fase clave para profesionalizar tus campañas de concienciación!

En este tema, desarrollaremos de forma práctica todo lo que hemos ido viendo en los capítulos anteriores, y analizaremos los resultados de las campañas, así que lo mejor, para desarrollar con más detalle el tema, es que veamos el siguiente video (**Obligatorio**).

 **Anti-Phishing con GoPhish, Campaign 2 - Charla 157** -
Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/9p-ul09HgZs>



7.8. GoPhish - Reporting

En esta charla nos centramos en una de las partes más importantes de cualquier campaña de concienciación: el **reporte y análisis de resultados**.

Veremos cómo debería responder un usuario al recibir este tipo de mails sospechosos. Desarrollaremos una potencialidad que nos presenta Gophish a través de "Report id" por medio de "Reporting Setting", tema que aún está como PROTOTIPO, pero ya lo dejamos presentado para que lo vayáis teniendo en cuenta, por otro lado, dejamos también planteada la duda: ¿está bien que en el mismo mail, le insertemos este tipo de mensajes, o no? (tema bastante discutido y discutible en este tipo de campañas...).

Aprende cómo interpretar los datos recolectados por GoPhish y cómo presentarlos de manera clara para generar valor dentro de tu organización.

En esta tema verás:

- Cómo interpretar los informes de GoPhish
- Métricas clave: apertura, clics, capturas y reportes de usuarios
- Consejos para presentar resultados a dirección o al equipo

¡Transforma datos en decisiones con reportes claros y accionables!

Nuevamente, este tema es eminentemente práctico por lo que directamente lo veremos en el siguiente video (**Obligatorio**).



info@darfe.es

🌐 **Anti-Phishing con GoPhish, Reporting - Charla 158** -
Aprendiendo Ciberseguridad paso a paso

https://youtu.be/f_xb4X_kgEQ

