CAMPAÑA DE PHISHING SIMULADO

¿QUÉ ES EL PHISHING?

El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Un ataque de phishing puede tener graves consecuencias para la empresa, ya que puede ocasionar la pérdida de información confidencial y financiera, dañar la reputación de la empresa y provocar interrupciones en los procesos de negocio. Además, la empresa puede enfrentarse a sanciones y multas por incumplimiento de las leyes y regulaciones de protección de datos.

Por lo tanto, es importante tomar medidas para protegerse contra los ataques de phishing y asegurarse de que sus empleados estén informados sobre cómo identificar y evitar este tipo de fraude.

Desde ABF Ciberseguridad, proponemos realizar una acción de phishing simulado en los socios del Clúster consistente en poner a prueba el nivel de madurez de los usuarios por medio de una campaña de correos electrónicos y entrega de los resultados obtenidos.

Esta acción se realiza en un entorno controlado y sobre un número determinado de cuentas de correo facilitados por la empresa participante y recomendamos que el conocimiento de esta iniciativa se reduzca al mínimo número de personas en la empresa (si es posible solo al CEO de la organización).

Precio de la acción

Dependiendo del número de usuarios, los precios son los siguientes:

Hasta 50 buzones	Hasta 100 buzones	Hasta 250 buzones	Hasta 500 buzones	> 500 buzones
25 €	23€	21€	19€	A consultar
Usuario	Usuario	Ususario	Usuario	

ABF CIBERSEGURIDAD y SISTEMAS

PROCEDIMIENTO

En un periodo establecido de tiempo de 3 meses se realiza el envío de un correo trampa a las direcciones de correo que nos ha facilitado la empresa.

Este correo puede adquirir diferentes formas de engaño por medio del uso de técnicas de phishing (suplantación de una cuenta conocida, de una entidad, de un proveedor, etc.).

Tras un primer informe de resultados, el usuario dispone durante 1 mes de una formación online en nuestra plataforma.

El tercer mes se realiza otro ataque de phishing para comprobar el aprendizaje de los usuarios.

Una vez realizada la acción facilitamos a la dirección de la empresa los resultados obtenidos con los que puede valorar el nivel de madurez de sus empleados.

El objetivo es comprobar el grado de concienciación en ciberseguridad de los usuarios de cuentas de correo corporativas ante esta técnica, muy usada por los atacantes, y que puede llegar a provocar gravísimos daños en la reputación de la compañía o en su cuenta de resultados.

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

AENOR ER Seguridad Información UNE-ISO/IEC 27001

BENEFICIOS DEL PHISHING SIMULADO

Realizar simulacros nos sirve para detectar posibles fallos, así como para formar al personal de la empresa y reforzar los conocimientos aprendidos.

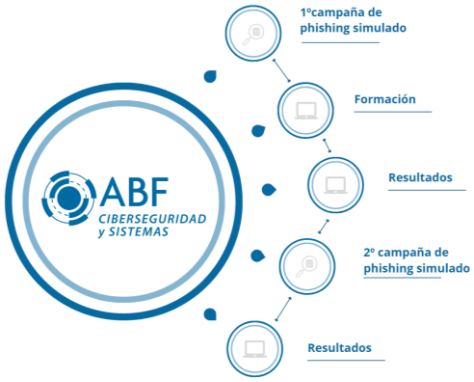
1. Protección de la información confidencial: Una campaña de phishing simulado ayuda a proteger la información confidencial de la empresa, como contraseñas, información financiera y datos de clientes, de ser robada o utilizada de manera indebida.
2. Evitar daños a la reputación: Las campañas de phishing pueden dañar gravemente la reputación de una empresa si se descubre que ha sido víctima de un ataque.
3. Prevenir interrupciones en los procesos de negocio.
4. Cumplimiento de leyes y regulaciones: Las empresas pueden enfrentar sanciones y multas por incumplimiento de leyes y regulaciones de protección de datos si son víctimas de un ataque de phishing.
5. Mejora de la seguridad: Una campaña de phishing simulado puede mejorar la seguridad general de la empresa al ayudar a proteger contra este tipo de fraude y aumentar la concienciación de los empleados.

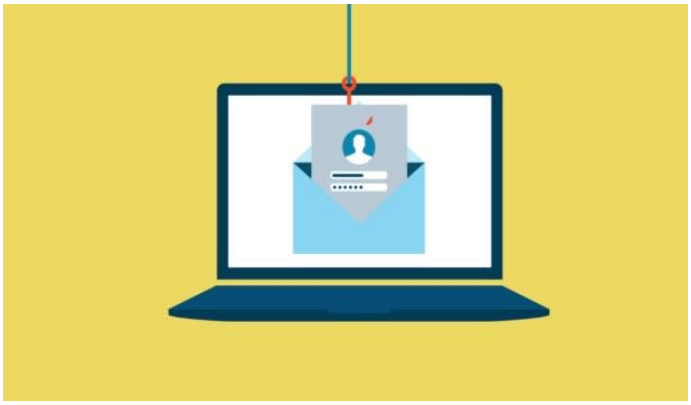
Estas acciones de Phishing simulado permiten a sus empleados tomar decisiones de seguridad más inteligentes, todos los días. Ahora puede capacitar y probar a sus usuarios para que detecten y comprendan el phishing.

a) Entrenar a los usuarios: Mediante nuestra amplia biblioteca de contenido en video actualizada a diario sobre conciencia de seguridad.

b) Probar a los usuarios con campañas de phishing simulado: para medir los conocimientos aprendidos de los usuarios se envían pruebas de phishing. Phishing simulados totalmente automatizados y con plantillas que se pueden adaptar o regionalizar.

c) Analizar los resultados: estadísticas e informes gráficos de alto nivel, incluso tendrá una línea de tiempo por cada usuario, grupo o departamento.





ABF CIBERSEGURIDAD Y SISTEMAS

PROTEGEMOS TUS REDES, PROTEGEMOS TUS DATOS

Telf: 941 10 70 80

comercial@abfsistemas.es

www.abfsistemas.es