

CHECKLIST RÁPIDO para crear su primera campaña de PHISHING



Para establecer una línea base de comportamiento de los usuarios de la organización es fundamental lanzar simulaciones de Phishing y luego, analizar los resultados. Pero, ¿por dónde empezar?

1 Alcance y Autorización

- ☐ Establezca el alcance y los objetivos de su campaña de simulación de Phishing.
- ☐ Asegúrese de solicitar autorización explícita dentro de la organización para realizar este tipo de evaluaciones.

2 Contenidos

- ☐ Defina la temática del escenario de simulación de Phishing.
- ☐ Elabore un contenido que responda a la temática definida. Un contenido se conforma de un correo electrónico y una página de destino con un formulario web. Considere:
 - ✓ Utilizar variables que identifiquen datos del usuario o la organización.
 - ✓ Disponibilizar el contenido en múltiples idiomas.
 - ✓ Dejar pistas que permitan a sus usuarios identificar el contenido como un Phishing.
 - ✓ Utilizar temáticas de interés y actualidad (puede tomar como base un Phishing real).
- ☐ Si el escenario de simulación de Phishing seleccionado posee temas sensibles y/o afectan a un área en particular, evalúe el impacto y solicite autorización explícita.

3 Herramienta de simulación

Una simulación de Phishing puede realizarse utilizando una plataforma en la nube especializada o bien, instalando una herramienta on premise en la infraestructura de la organización.

Herramienta on premise en infraestructura propia

- ☐ Configure una cuenta de correo en un servidor SMTP que brinde la posibilidad de hacer Spoofing.
- ☐ Configure un servidor web para alojar la página de destino de la simulación de Phishing.
- ☐ Aplique las medidas de seguridad pertinentes en ambos servidores para proteger la seguridad de la información.
- ☐ Adquiera y configure dominios para envío de correos de simulación de Phishing y para navegación web del sitio de Phishing simulado.
- ☐ Adquiera y configure certificados SSL para los dominios y configure además sus registros SPF, DKIM y DMARC.
- ☐ Elabore un plan de contingencia para los dominios de simulación que caigan en listas negras globales.
- ☐ Elabore y siga un procedimiento de actualización y hardening de la infraestructura definida.
- ☐ Como recomendación, asegúrese de elegir una herramienta que automatice todo el ciclo de vida de la simulación:
 - ✓ Calendarización de la campaña.
 - ✓ Envío de correos.
 - ✓ Registro de interacciones de los usuarios.
 - ✓ Reporting de resultados en tiempo real.
 - ✓ Recolección de registros de auditoría inalterables.
 - ✓ Identificación y ocultado de falsos positivos.

Plataforma en la nube

- ☐ Seleccione una herramienta de simulación de Phishing adecuada para sus necesidades.
- ☐ Audite las características de seguridad de la herramienta para proteger su información.



4 Whitelist

- ☐ Identifique las herramientas de seguridad de la organización involucradas en la recepción de correos y navegación web.
- ☐ Utilice las opciones de whitelist de dichas herramientas para:
 - ✓ Asegurar la correcta recepción en la bandeja de entrada del usuario de los correos de simulación de Phishing (para que no se marquen como SPAM).
 - ✓ Evitar que las herramientas interactúen con los correos, generando falsos positivos en estadísticas de simulación.
 - ✓ Asegurar la correcta visualización y navegación de la página de destino del Phishing simulado.
- ☐ Opcionalmente, configure el cliente de correo para que muestre las imágenes del correo de simulación de Phishing, sin que el usuario deba autorizarlo. Esto favorece la detección de apertura de correos pero, al mismo tiempo, puede llamar la atención del usuario si no está acostumbrado a visualizar automáticamente las imágenes de los correos recibidos.
- ☐ Para asegurarse que todo funcione satisfactoriamente, lance campañas de prueba hasta conseguir que:
 - ✓ El correo sea recibido en la bandeja de entrada.
 - ✓ La página de destino se pueda navegar correctamente.
 - ✓ Las estadísticas se correspondan con las acciones de prueba realizadas.
 - ✓ No haya falsos positivos o, si existen, sean filtrados.
 - ✓ Las imágenes se descarguen sin autorización, si así desea.



5 Lanzamiento

- ☐ Defina la duración de la campaña. Es recomendable no extender la simulación por más de 48 horas¹.
- ☐ Elabore un conjunto de campañas de simulación de Phishing a lo largo de un determinado período y analice todos los resultados, pues una única simulación no es suficiente para diagnosticar la línea base del comportamiento de sus usuarios².

6 Progreso

- ☐ A partir de la línea base, plantee objetivos y metas para el programa de concientización de su organización.
Programa campañas de concientización utilizando diferentes recursos como Módulos Interactivos, Newsletters, Videos, Videojuegos, Webinars, Pósters y sesiones presenciales.
- ☐ Vuelva a medir de manera periódica su línea base para evaluar la efectividad de sus acciones y demostrar el cambio de comportamiento.

Nota

Existen partners integradores que prestan servicios gestionados y llevan adelante tanto campañas de simulación de Phishing como completos programas de concientización. Esto permite al CISO delegar o tercerizar las acciones tácticas y operativas listadas en este documento, manteniendo la parte estratégica en sus manos.



1 [¿Cuánto duran las campañas de Phishing?](#)

2 [La simulación de Phishing de oro, o cómo interpretamos de manera incorrecta los resultados de nuestras pruebas.](#)