LA HERRAMIENTA

📊 El Dashboard de GoPhish

Una vez que lanzas una campaña de phishing, GoPhish comienza a recolectar datos en tiempo real. El Dashboard es tu centro de comando para entender qué está pasando.

🖥️ ¿Qué ves en pantalla?

Al entrar a la campaña activa, verás una serie de tarjetas con números grandes. Cada una representa una etapa del embudo de engaño:

- **Emails Sent:** Correos que el servidor SMTP aceptó y envió.
- **Emails Opened:** Personas que abrieron el correo (se rastrea con el píxel `{{.Tracker}}`).
- **Link Clicked:** Personas que hicieron clic en el enlace malicioso.
- **Data Submitted:** Personas que introdujeron datos en la Landing Page.
- **Email Reported:** Personas que marcaron el correo como spam o lo reportaron a TI (¡esta es la métrica más importante!).

> 💡 **Dato Clave**
>
> GoPhish también te permite ver el detalle por usuario. Si haces clic en "View Details", puedes ver exactamente quién abrió el correo, a qué hora, y si introdujo datos. Esto es vital para personalizar la capacitación.

ANÁLISIS

📈 Interpretando las Métricas (El Embudo)

No todos los que reciben el correo caen en la trampa. El flujo es un embudo y cada paso tiene un significado distinto para la seguridad de la empresa.

🔽 El Embudo del Phishing

ETAPA	¿QUÉ SIGNIFICA?	NIVEL DE RIESGO
Enviado	El correo llegó a la bandeja de entrada.	Neutro (es el punto de partida).
Abierto	El usuario vio el correo. No hizo clic, pero prestó atención.	Bajo. Es normal abrir correos.
Clic	El usuario hizo clic en el enlace. Ya está en la página falsa.	**Medio-Alto**. Demuestra falta de criterio para verificar enlaces.
Datos Enviados	El usuario introdujo su usuario y contraseña.	**Crítico**. La cuenta está comprometida.
Reportado	El usuario sospechó y reportó el correo.	**Excelente**. Es el comportamiento ideal.

📉 Ejemplo de una Campaña Real (100 empleados)

Imagina que enviaste el correo a 100 empleados. Los resultados podrían ser:

- **100 enviados.**
- **60 abiertos (60%).** Es una tasa normal.
- **25 clics (25%).** Un cuarto de la empresa cayó en la trampa.
- **10 datos enviados (10%).** 10 cuentas comprometidas.
- **5 reportados (5%).** Solo 5 personas tuvieron el criterio de reportar.

En este escenario, el **25% de clic** y el **10% de datos enviados** son cifras alarmantes que justifican una capacitación inmediata. El **5% de reporte** es demasiado bajo; la empresa necesita fomentar una cultura de "si dudas, repórtalo".

CUANTIFICACIÓN

🧮 Cálculo del Riesgo Humano

Los números fríos no siempre convencen a la gerencia. Necesitas traducir esos porcentajes a un lenguaje de riesgo empresarial.

📐 Fórmula del Riesgo de Phishing

Puedes usar esta fórmula simple para calcular el riesgo:

Fórmula

```
Riesgo = (Tasa de Clics + Tasa de Datos Enviados) / 2
```

Siguiendo el ejemplo anterior: `(25% + 10%) / 2 = 17.5%`. Un riesgo del 17.5% significa que, en promedio, 1 de cada 6 empleados comprometería las credenciales de la empresa ante un ataque real.

💰 Traducción a Impacto Financiero

Si un atacante real compromete 10 cuentas, el costo promedio de una brecha de datos (según IBM) es de **$4.45 millones de dólares** a nivel global. Para una Pyme, puede ser desde **$50,000 hasta $500,000 USD** dependiendo del sector.

Tu informe debe decir: *"Si esta campaña hubiera sido un ataque real, la empresa habría perdido X cuentas, con un impacto estimado de $Y dólares"*.

ENTREGABLE

📝 El Informe de Auditoría (Lo que entregas al cliente)

GoPhish te permite exportar los resultados en CSV. Pero un buen hacker ético no entrega un CSV; entrega un informe ejecutivo con conclusiones y recomendaciones.

📄 Estructura del Informe Profesional

1. **Resumen Ejecutivo:** Un párrafo con las 3 métricas clave (Clics, Datos, Reportes) y la conclusión principal.
2. **Metodología:** Explicar que se usó GoPhish, qué plantilla se usó, cuántos usuarios participaron, y qué tipo de Landing Page se creó.
3. **Resultados Detallados:** Las tablas y gráficos del Dashboard.
4. **Análisis de Riesgo:** La fórmula aplicada y el impacto potencial.
5. **Recomendaciones:** Plan de acción (capacitación, 2FA, filtros de correo).

🚨 La Cláusula de Confidencialidad

Al final del informe, debes incluir una cláusula legal que diga:

> **Cláusula**
>
> "Los datos aquí presentados son confidenciales y producto de una simulación autorizada. Las credenciales capturadas fueron eliminadas de forma segura después del análisis. Este informe no debe ser compartido fuera de la organización."

ACCIÓN

🎓 Plan de Concienciación (El Verdadero Objetivo)

La simulación no sirve de nada si no se traduce en aprendizaje. Aquí es donde le das valor real a la empresa.

📚 Diseño de la Capacitación

Dependiendo de los resultados, tu plan debe incluir:

- **Para los que hicieron clic pero no enviaron datos:** Un correo automático o un micro-video explicando cómo identificar enlaces sospechosos (pasar el ratón por encima, revisar el dominio, etc.).
- **Para los que enviaron datos:** Una sesión de 15 minutos explicando qué es el Phishing y cómo usar gestores de contraseñas para no reutilizarlas.
- **Para los que reportaron:** Un correo de felicitación. Fomentar el comportamiento positivo es clave para que la próxima vez más gente reporte.

📅 Campañas de Seguimiento

La concienciación es un proceso continuo. Recomienda a la empresa:

- Hacer una simulación cada 3 meses con plantillas diferentes (ahora un banco, ahora un proveedor, ahora un paquete de envío).
- Medir el progreso: El objetivo es que la tasa de reporte suba del 5% al 20% o 30%, y la tasa de clics baje del 25% al 5%.

EVOLUCION

🛡️ Métricas de Éxito a Largo Plazo

Un programa de concienciación maduro no se mide por cuántas personas caen, sino por cuántas personas detectan y reportan los ataques.

📈 El KPI Clave: Tasa de Reporte

La métrica más importante de un programa de seguridad no es la de clics, sino la de **Email Reported**. Si un empleado recibe un correo sospechoso y lo reporta al equipo de TI, ese correo puede ser analizado, bloqueado y se puede alertar a toda la empresa.

Tu objetivo como pentester es que, con el tiempo, la tasa de reporte supere el 20%.

🔬 El Botón de Reporte (Phish Alert)

Recomienda a la empresa instalar un botón de "Reportar Phishing" en Outlook o Gmail. Herramientas como **KnowBe4** o **Microsoft Defender** incluyen esta función. Esto empodera al empleado y convierte a la primera línea de defensa en un sensor activo.

🎓 ¡Fin de la Clase 3.4!

Ya sabes cómo medir, analizar y comunicar los resultados de una campaña de phishing. En la próxima clase (3.5) haremos el Proyecto Final, donde ejecutarás una simulación completa de principio a fin y presentarás tu informe de hallazgos.