SMARTFENSE

6 BUENAS PRÁCTICAS
PARA SIMULAR PHISHING

SMARTFENSE

1. **Planifica antes de lanzar**

➜ Define el objetivo de la simulación.
↳ *¿Qué comportamiento quieres observar o modificar?*

➜ Revisa tu proceso de whitelisting.

➜ Comienza con campañas de prueba.

SMARTFENSE

2. **Que no caiga todo el mundo**

➜ Haz que tus simulaciones se parezcan a casos reales.

➜ El objetivo no es hacer caer a la mayoría, sino aprender del comportamiento real.

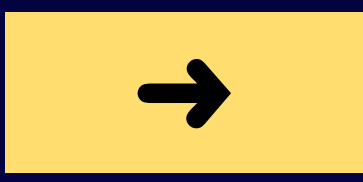
SMARTFENSE

3. **Varía, mide y aprende**

➜ Envía varias simulaciones por mes.

↳ *Cambia el tema, el día, el horario, los grupos destinatarios, el grado de personalización.*

➜ Agrupa resultados por campaña para tener una visión más clara.



SMARTFENSE

4. **No pierdas tiempo donde no hace falta**

➜ Usa plantillas predefinidas.

↳ *Si editas, hazlo de forma mínima y estratégica.*

➜ Solo en casos especiales vale la pena clonar ataques reales.

➜ No diseñes campañas buscando “hacer caer” a los usuarios.

↳ *Eso solo distorsiona tus métricas.*

➜

SMARTFENSE

5. **Conciencia en el momento exacto**

➜ Si alguien cae en la simulación, actívalo con un Momento Educativo.

↳ *Mostrar qué habría ocurrido en un ataque real es más efectivo que cualquier charla.*

SMARTFENSE

6. **Evalúa y ajusta**

➜ Revisa los resultados.

➜ Si algo no salió como esperabas, ajusta tus objetivos, revisa la whitelist, lanza nuevas pruebas.

SMARTFENSE

Simular bien no es hacer más,
es hacerlo mejor.

Cada simulación
debe enseñarte algo nuevo.

Sigue estas prácticas para mejorar tus simulaciones

¡Déjanos tus dudas en comentarios!

SMARTFENSE

www.smartfense.com
info@smartfense.com