CIBERSECTO
SEGURIDAD DIGITAL

// HERRAMIENTAS DE ATAQUE · MÉXICO 2026

GUÍA DE PROTECCIÓN

¿Qué es SEToolkit?
La herramienta que clona tu banco.

El Social-Engineering Toolkit es un framework de código abierto usado en pruebas de penetración para simular ataques de ingeniería social. El problema: cualquiera puede descargarlo gratis, no solo los pentesters.

01 — QUÉ HACE REALMENTE

🖥️ **Clona páginas web en segundos**

Copia el login exacto de Facebook, Gmail, un banco o cualquier sitio, pixel por pixel. El atacante la sube a un servidor y la disfraza con un enlace parecido al original.

📧 **Genera campañas de phishing masivo**

Automatiza el envío de correos o mensajes con el enlace clonado, incluyendo plantillas que imitan bancos, redes sociales y servicios de streaming.

🎭 **Ataques combinados (multi-attack)**

Puede combinar clonación web + archivo infectado + captura de credenciales en un solo ataque, todo desde una terminal de Kali Linux sin escribir código propio.

02 — CÓMO LLEGA A TI

CASO 01

Enlace "de tu banco"

Un SMS o WhatsApp dice que tu cuenta se bloqueó. El enlace lleva a una página clonada con SEToolkit, idéntica a la de tu banco real.

CASO 02

"Ganaste un premio"

Página clonada de una rifa o promoción pide tu login de redes sociales para "verificar tu identidad" antes de entregarte el premio.

CASO 03

Soporte técnico falso

Llamada o chat que te dirige a un "portal de verificación" clonado para que ingreses usuario y contraseña de tu correo corporativo.

CASO 04

WiFi público gratuito

Red WiFi abierta cuyo portal de "inicia sesión para conectarte" es en realidad una página clonada que captura credenciales.

03 — SEÑALES DE UNA PÁGINA CLONADA

✓ **La URL no coincide exactamente** con el dominio oficial (letras cambiadas, guiones extra, dominio .xyz en vez de .com).

✓ **Pide datos que el sitio real nunca pide juntos** — usuario, contraseña y código de verificación en la misma pantalla.

✓ **No tiene candado HTTPS válido** o el certificado pertenece a otro dominio distinto al que dice ser.

✓ **Llegaste ahí por un enlace**, no escribiendo tú mismo la dirección en el navegador.

// REGLA DE ORO

Si llegaste al login por un enlace que no escribiste tú, asume que es falso hasta comprobar lo contrario.

Escribe la dirección manualmente en el navegador o usa la app oficial. Nunca inicies sesión desde un enlace recibido.