ALERTA ACTIVA

CONCIENTIZACION · QRISHING

ESE CODIGO QR puede ser veneno digital

Escaneas el QR del menu, del estacionamiento, del cajero — y en segundos estas en un sitio falso que roba tus datos bancarios. Sin que lo notes.

3s	400%	$2
tarda el ataque en redirigirte	mas ataques QR en LATAM vs 2022	pesos cuesta hacer el ataque

01 — ASI FUNCIONA EL ATAQUE

Lo que pasa cuando escaneas ese QR

01 — Pegan un QR falso encima del original

En restaurantes, estacionamientos, farmacias y oficinas. Una calcomanía de $2 pesos encima del codigo legitimo. Visualmente identico al original — imposible de distinguir a simple vista.

02 — Te redirigen a un sitio clonado 100% real

Mismo logo, mismos colores, mismo formulario. Tu telefono no te avisa nada. La pagina falsa es copia exacta del banco o servicio que esperabas encontrar.

03 — Ingresas tus datos y se los envias al atacante

Usuario, contrasena, numero de tarjeta, CVV — en tiempo real. Tu crees que pagaste el estacionamiento. Ellos ya tienen acceso completo a tu cuenta bancaria.

02 — DONDE OCURRE EN MEXICO

Los lugares mas comunes del ataque

Restaurantes y cafes
QR de menu o pago en mesa. Facil de reemplazar con calcomanía. El cliente nunca revisa el codigo antes de pagar.
RIESGO ALTO

Estacionamientos
Objetivo favorito: montos altos, urgencia real, nadie supervisa los letreros de pago al salir.
RIESGO MUY ALTO

Oficinas de gobierno
El contexto oficial baja la guardia. La victima confia mas porque parece institucional y legitimo.
RIESGO ALTO

OXXO y tiendas
Trafico muy alto = mas victimas por dia. El atacante no necesita estar presente en el lugar.
RIESGO ALTO

Paqueteria falsa
QR en sobres de FedEx, DHL o Correos clonados. Rastreo falso que roba credenciales. Creciendo en 2026.
CRECIENDO 2026

Hoteles
Check-in, WiFi y servicios por QR. El huesped esta distraido y confia ciegamente en el entorno.
VIGILAR

03 — 4 HABITOS QUE TE PROTEGEN SIEMPRE

Lo que haces desde hoy

01
Lee la URL antes de abrir
Tu camara muestra la URL antes de abrir el enlace. Si el dominio es raro o no corresponde al lugar, cierra sin entrar.

02
Toca el QR fisicamente
Si hay una calcomanía pegada encima del QR original, se nota al tacto o se despega. Es la senal mas clara de ataque.

03
Nunca des datos por un QR
Si necesitas pagar, entra directo a la app de tu banco. Nunca uses el formulario al que te llevo el codigo escaneado.

04
Desactiva apertura automatica
Configura tu camara para que muestre la URL y pida confirmar antes de abrir. iOS y Android lo permiten en ajustes.

REGLA DE ORO

Si el QR te pide datos bancarios, contrasena o informacion personal — para. Ese dato no se ingresa jamas desde un codigo escaneado en la calle. Entra siempre directo a la app oficial.

NAVI · Cibersecto
CIBERSEGURIDAD · IA · MEXICO

navi-site-3h8.pages.dev
instagram.com/cibersecto
tiktok.com/@cibersecto
facebook.com/cibersecto