Anatomía de un Email Seguro y Protocolo de Emergencia

Cómo detectar la amenaza invisible y qué hacer cuando el escudo falla.

ProTech Academy - Ciberseguridad


90%
El 90% de los ciberataques inician aquí
Los atacantes no necesitan romper un firewall complejo; solo necesitan que tú hagas un clic.
Key Insight:
El 'Phishing' es lanzar miles de anzuelos digitales esperando que alguien muerda. Tu intuición es la barrera final.

El Semáforo de Seguridad

Antes de actuar, evalúa las tres zonas de riesgo.

Zona Roja: ¿Quién lo envía realmente?

Zona Amarilla: ¿Qué emociones intenta provocar?

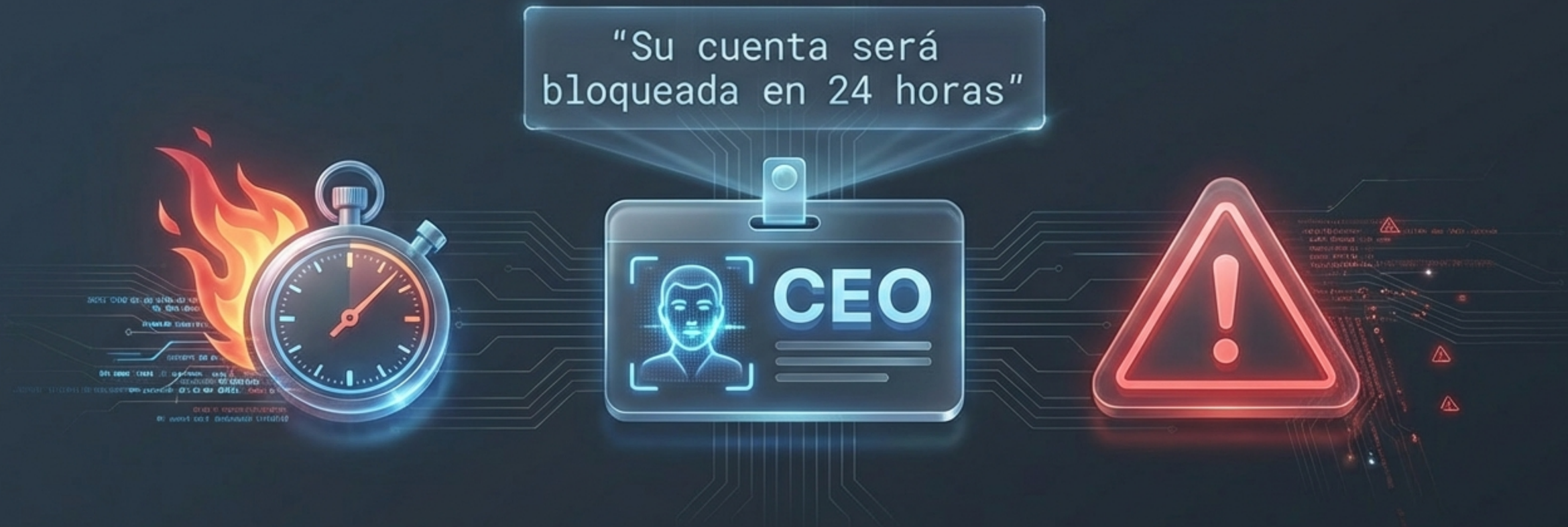
Zona Crítica: ¿A dónde te lleva?

Zona Roja: La Máscara del Remitente

Los atacantes usan el 'Typosquatting' (errores tipográficos intencionales) para engañar a tu cerebro.

Verifica siempre el dominio exacto, no solo el nombre que muestra el correo. Un cero no es una letra 'o'.

Zona Amarilla: El Anzuelo Psicológico



Si un correo apela a emociones fuertes o te pide actuar *YA*, detente.

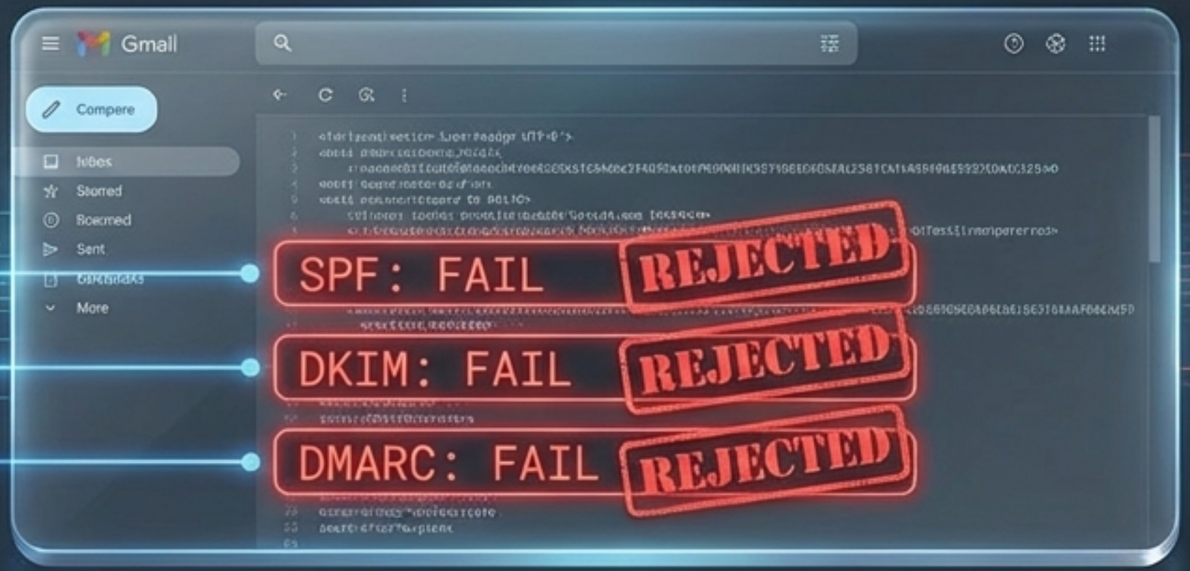
La ingeniería social busca desactivar tu pensamiento crítico mediante el pánico o la falsa autoridad.

La Regla de Oro: ‘Hover before you click’

Pasa el mouse antes de hacer clic. La verdadera dirección siempre se revela al pasar el cursor.

Si ves un enlace acortado (bit.ly) o un dominio que no coincide con el remitente, es una trampa.

Lo Invisible: El ADN Técnico

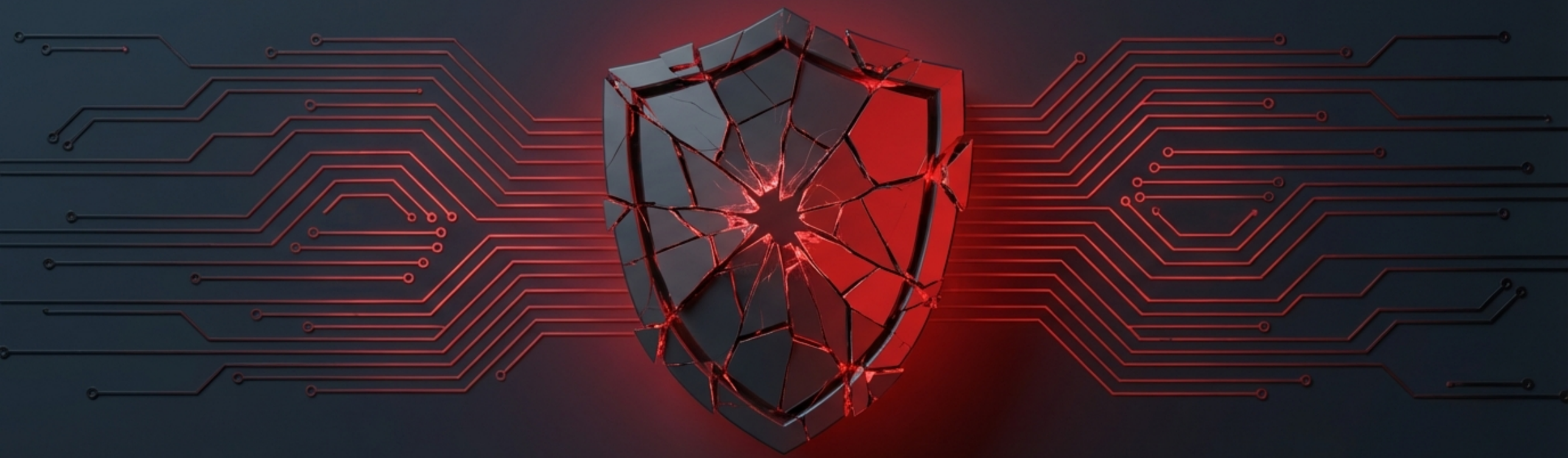


SPF y DKIM son como pedirle la cédula al cartero. Verifican si el servidor tiene permiso real para enviar ese correo.

En caso de duda, revisa las cabeceras. Si dice 'FAIL', es una suplantación garantizada.

¿Hiciste Clic?

No entres en pánico. Actúa.



La diferencia entre un incidente menor y un desastre total son los primeros 5 minutos.

Paso 1: Cortar la Conexión

Aísla el equipo inmediatamente.
Desconecta el cable de red o apaga el Wi-Fi.

El malware necesita internet para recibir
órdenes o robar datos.

Paso 2: Preservar la Escena

NO APAGUES EL EQUIPO.

La memoria RAM contiene evidencia forense vital que se pierde al apagar. Déjalo encendido pero desconectado de la red.

Paso 3: Contención Externa

Usa un dispositivo diferente (tu celular con datos móviles) para cambiar las contraseñas críticas: Correo, Banco, CRM.

El atacante podría tener ya tus claves.

Paso 4: Reportar sin Miedo

“Reportar salva, ocultar condena.”

Reportar un error a los 5 minutos es un incidente manejable. Ocultarlo por vergüenza puede destruir la empresa. La honestidad es seguridad.

Tú eres el “Firewall Humano”

La tecnología ayuda, pero tu criterio es la última barrera.

Verifica siempre (Anatomía), duda de la urgencia y reporta al instante si fallas (Plan de Emergencia).
¿Estás listo para el Quiz Final?

Preguntas y Examen

ProTech Academy