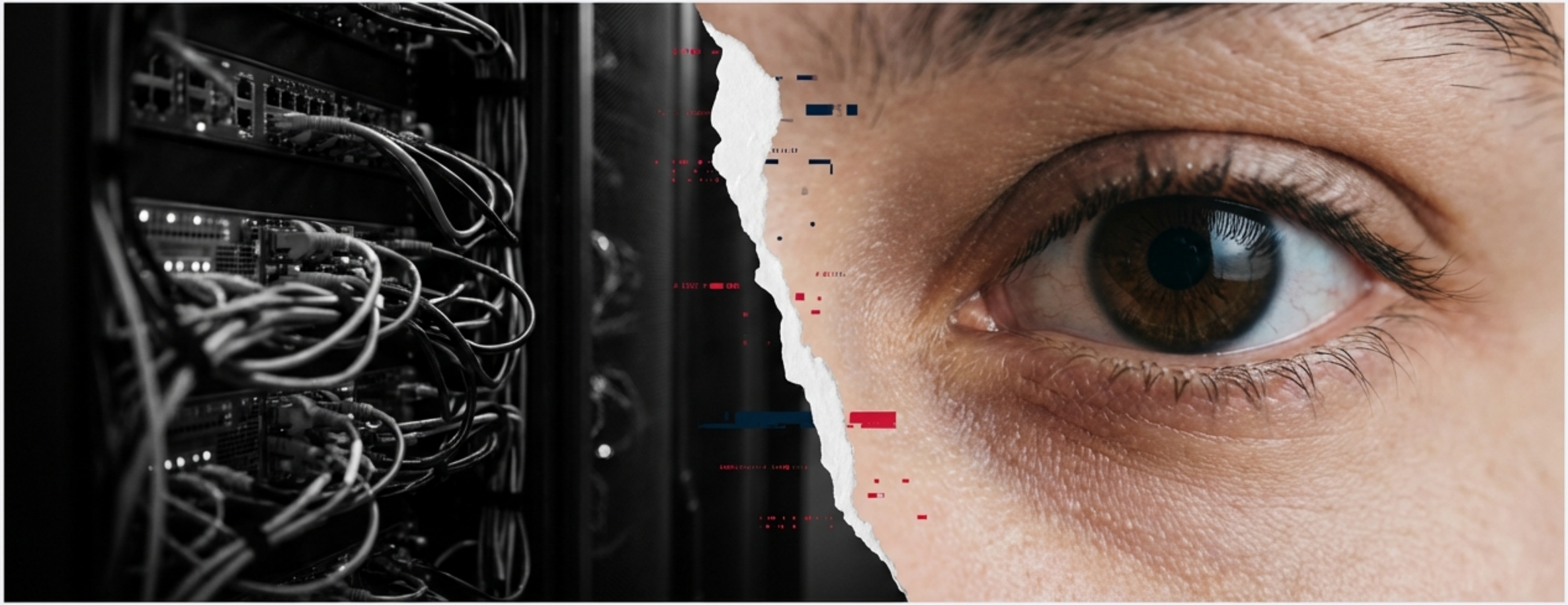
No hackeamos computadoras. Hackeamos personas.

Ingeniería Social, Psicología y Defensa Corporativa.



El Firewall no importa si tú abres la puerta.

90%

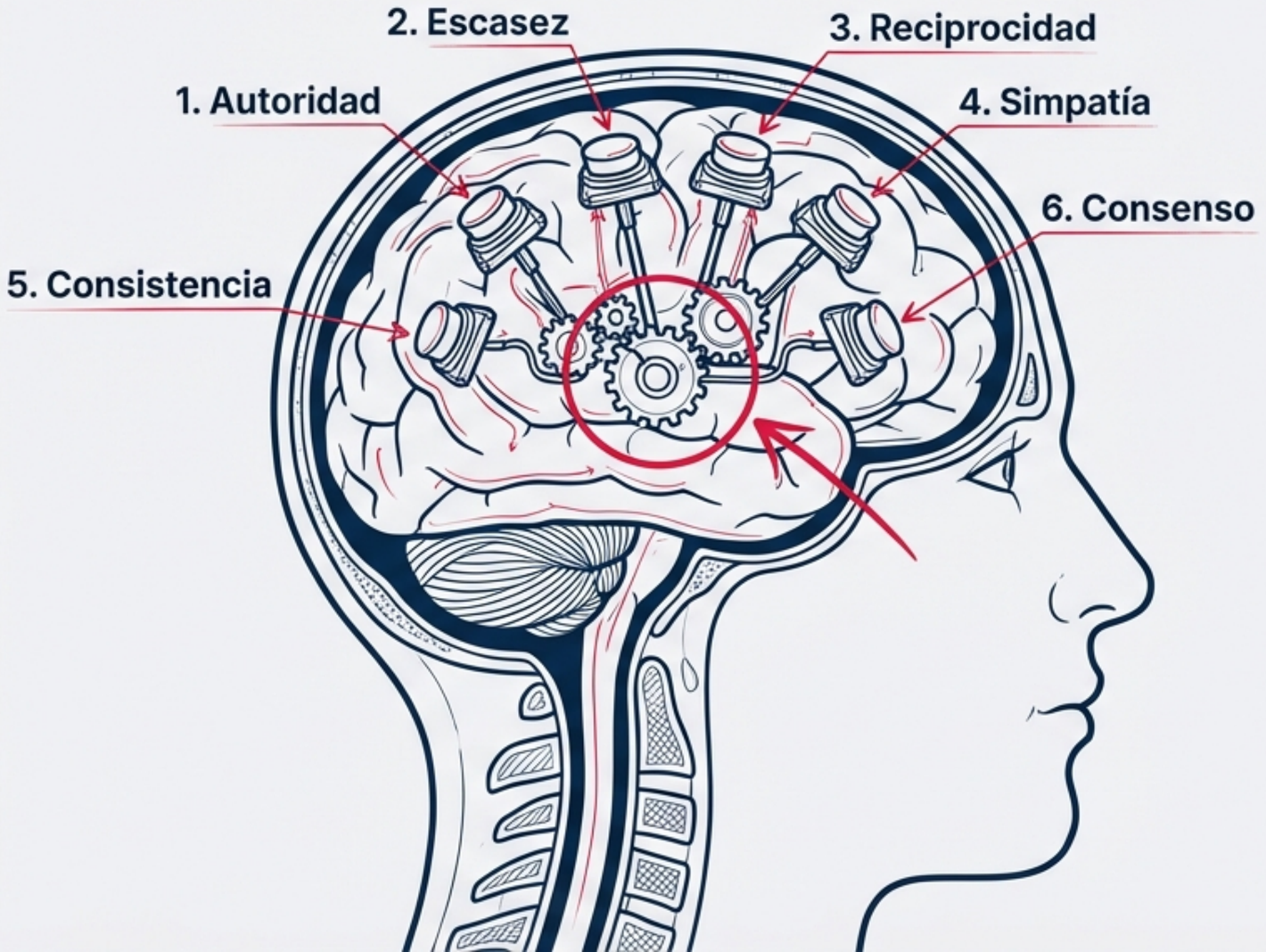
El **90%** de los ciberataques exitosos inician con un email.

Los delincuentes no rompen la seguridad; esperan a que tú los invites a pasar.

Ingeniería Social: La manipulación de la confianza.

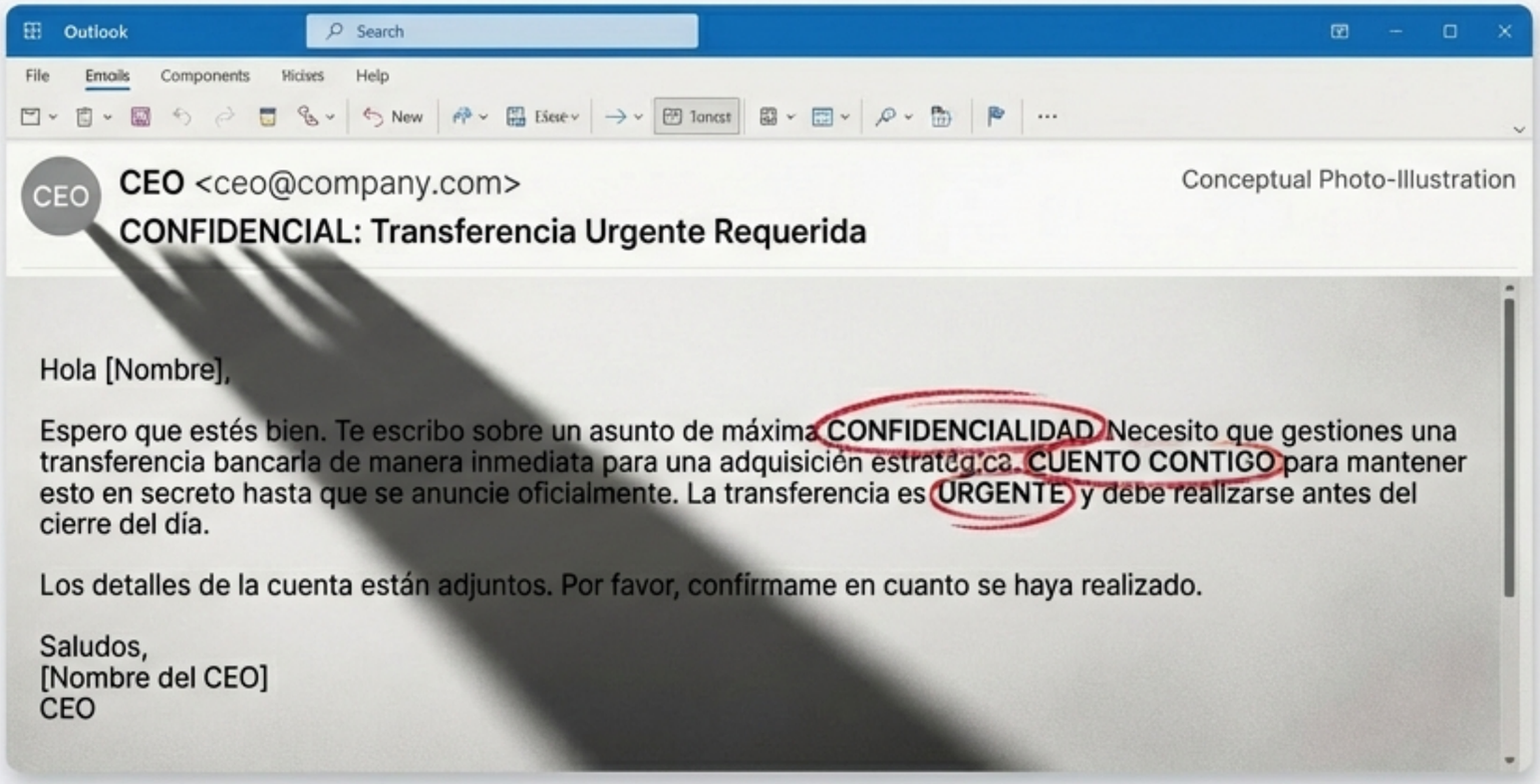
- **Definición:** El arte de engañar a las personas para que revelen información confidencial.
- **El objetivo:** Desactivar tu pensamiento crítico y activar tu obediencia automática.
- **No buscan tu contraseña por fuerza bruta, buscan que tú se la entregues.**

Los 6 Botones de la Influencia (Robert Cialdini).



1. **Autoridad:** Obedecemos al jefe.
2. **Escasez:** Tememos perder la oportunidad.
3. **Reciprocidad:** Nos sentimos obligados a devolver favores.
4. **Simpatía:** Confiamos en quien nos cae bien.
5. **Consistencia:** Queremos ser coherentes.
6. **Consenso:** Seguimos a la manada.

Exploit #1: Autoridad (El Fraude del CEO).



El Escenario: Un correo urgente de la gerencia pidiendo una transferencia.

Los Disparadores:

- **Confidencial** (Te hace sentir especial).
- **Cuento contigo** (Presión emocional).
- **Rápido** (Evita que pienses).

Exploit #2: Escasez y Urgencia (El Pánico)

- **El Guion:** "Tu cuenta se va a bloquear" o "Acción requerida YA".
- **El Efecto:** El miedo desconecta el análisis lógico del cerebro.
- **La Trampa:** Crean un problema falso y te ofrecen la única solución rápida.

Exploit #3: Reciprocidad y Simpatía.

Soporte Técnico Falso: “Vi un error en tu equipo, déjame arreglarlo” (Te hacen un favor primero).

- **La Estafa de WhatsApp:** Explotan el vínculo emocional familiar.
- **Lección:** La amabilidad excesiva o la emergencia familiar digital son banderas rojas.

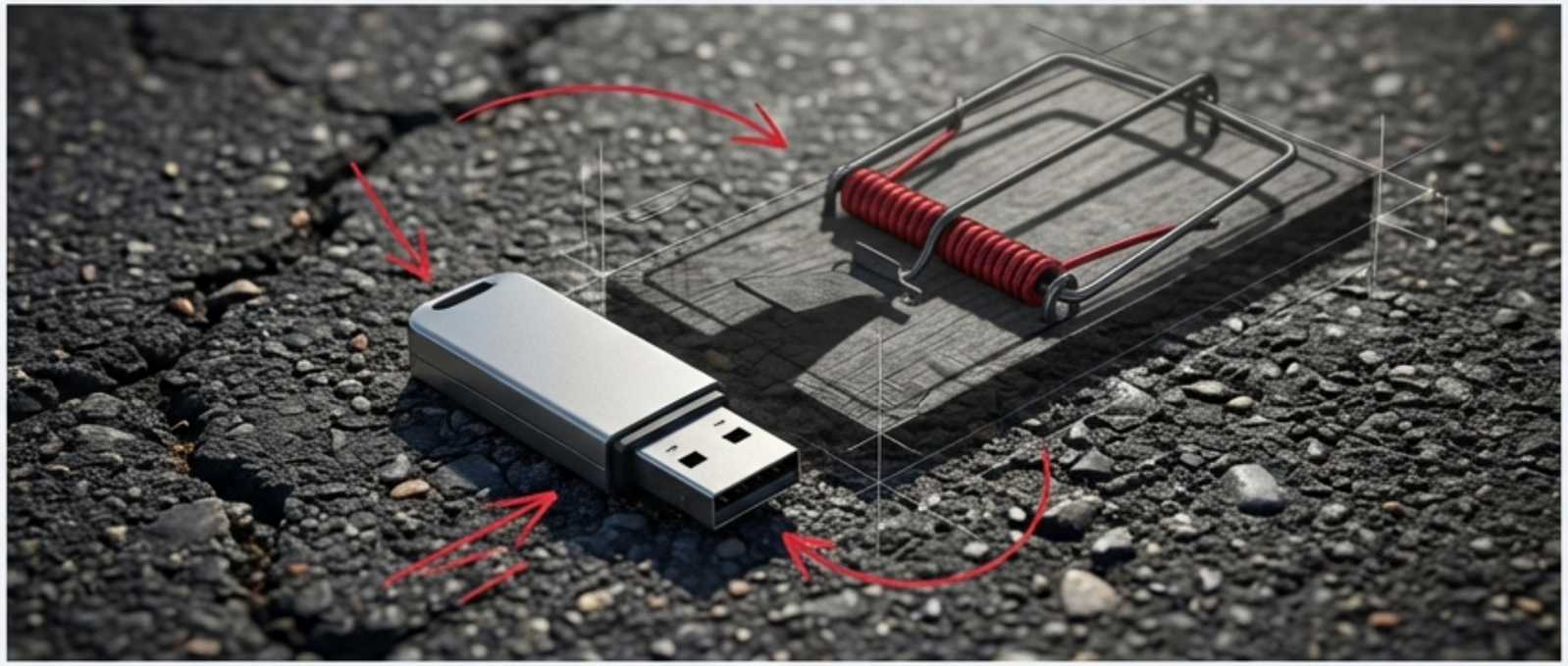
Caso Práctico: Vishing (La llamada)

- **El Atacante:** Genera urgencia y confusión auditiva.
- **La Solicitud:** Pide algo “simple” (un código) para resolver un problema “grande”.
- **Tu Defensa:** Nunca des códigos por teléfono. Cuelga y llama al número oficial.

Caso Práctico: El Acceso Físico (Piggybacking)

- **La Trampa de la Amabilidad:** Sostener la puerta a alguien “cargado”.
- **El Resultado**: Un extraño entra a las oficinas sin tarjeta de acceso.
- **La Regla**: Si no tienes tarjeta, no entras. La seguridad está por encima de la cortesía.

Caso Práctico: La Curiosidad (El USB Perdido)



- **El Escenario:** Encuentras un USB en el estacionamiento.
- **El Impulso:** '¿Qué fotos tendrá?'
- **La Realidad:** Al conectarlo, despiega malware automáticamente.
- **Acción:** No lo conectes. Entrégalo a TI inmediatamente.

Corporate Noir meets Editorial Journalism

Entrenamiento Visual: Encuentra las diferencias.

- **Typosquatting:** El cero engaña al ojo.
- **El Enlace Oculto:** El botón miente, el tooltip dice la verdad.
- **La Técnica:** Pasa el cursor sobre el enlace sin hacer clic. Esa es tu “pistola humeante”.

Tu Protocolo de Defensa: El Semáforo

ROJO (Detente): Remitente desconocido, dominio extraño, solicitud de claves.

AMARILLO (Precaución): Urgencia ('Hazlo YA'), errores ortográficos.

VERDE (Adelante): Solo si has verificado por un segundo canal.

Contra-Inteligencia: Confía, pero verifica.

- Si recibes una llamada del banco o soporte: **Cuelga y llama tú** al número oficial.
- Si el CEO pide una transferencia urgente: Escribe por Teams para confirmar.
- Verificar no es desconfianza, es profesionalismo.

¿Hiciste Clic? Tu Plan de Emergencia.

1. **Desconecta**: Quita el cable de red o apaga el Wi-Fi inmediatamente.
2. **NO Apagues**: Deja el equipo encendido para evidencia forense.
3. **Reporta**: Llama a TI ya.

"Reportar un error a los 5 minutos es un incidente. A los 5 días es un desastre."

Tú eres el Eslabón Fuerte.

La tecnología tiene límites. Tu intuición no.
Tu escepticismo saludable es el mejor antivirus de la empresa.
Mantente alerta. Protege nuestra información.