

■ SEGURIDAD

El Fraude Casi Nunca Empieza con un Hackeo

La imagen del atacante rompiendo un sistema es cómoda, porque deja el problema del lado de la tecnología. Lo que vemos casi siempre es más simple. Alguien escribe haciéndose pasar por un proveedor, por el banco o por un familiar, con datos suficientes para sonar real, y pide algo urgente.

Funciona porque se apoya en la prisa y en la jerarquía. Un mensaje que parece del dueño, un viernes a las seis, pidiendo un pago excepcional, rara vez se cuestiona.

Las Tres Puertas que Revisamos Primero

- El correo y el teléfono que recuperan todo lo demás. Si alguien entra ahí, el resto cae en orden.
- Quién puede autorizar un pago, y con qué confirmación fuera del canal donde se pidió.
- Qué información pública tuya y de tu familia hace fácil construir un mensaje creíble.

Verificar No Es Desconfiar

La regla que más resultados da también es la más aburrida. Toda solicitud de dinero o de acceso se confirma por un segundo canal acordado de antemano. Siempre, sin excepciones por rango ni por urgencia. En cuanto existe la excepción, al atacante solo le queda fabricar urgencia.

Conviene practicarla antes de necesitarla. Una llamada corta al número de siempre. Una frase acordada. Un segundo par de ojos por encima de cierto monto. Son acuerdos, no software.

Qué Cubre el Blindaje Ejecutivo

Revisamos cuentas y dispositivos de quien decide y, si lo acuerdan, de su familia. Reforzamos accesos y recuperación, bajamos la exposición pública que no hace falta, y dejamos por escrito qué hacer cuando algo se pierde o alguien sale de la empresa.

Son medidas para reducir riesgo y detectar antes. Ninguna elimina la posibilidad de fraude, y quien prometa lo contrario merece una segunda mirada.