¿Algo te huele raro?

Dónde mirar, en qué orden, y qué hacer si ya pasó. Los números de cada lista están puestos sobre el ejemplo.

ALERTA.SECPRO.CO Quiz y guía completa

SecPro
SECURITY PROFESSIONALS

UN CORREO

Míralo en este orden

↩ Responder ↪ Reenviar Eliminar

Nueva política de uso de IA — confirma tu acceso

1 **Tu Empresa · Seguridad de la Información**

2 <notificaciones@tuempresa-seguridad.co>

Estimado colaborador,

3 Los accesos no confirmados antes del martes a las 6:00 p.m. serán suspendidos automáticamente.

4 **Confirmar mi acceso**

5 Ingresa con tu usuario y contraseña corporativos para validar tu perfil.

1. **La dirección, no el nombre.** El nombre que aparece lo escribe quien envía. Ábrelo y lee la dirección real.
2. **El dominio, letra por letra.** Aquí sobra un guion. Una letra cambiada o un punto de más bastan.
3. **La prisa con fecha límite.** La urgencia está puesta para que actúes antes de verificar.
4. **El enlace.** Pasa el cursor por encima y lee a dónde va de verdad. El texto del botón no prueba nada.
5. **Si pide usuario y contraseña, ya está.** Ninguna entidad legítima lo pide por correo. Ninguna.

UN JEFE POR TEAMS O WHATSAPP

Nadie tuvo que hackear nada

CR **Carlos Restrepo** 1 EXTERNO 2
c.restrepo@tuempresa-corp.net

Hola, buenos días. ¿Estás ocupado ahora?
8:04 a.m.

3 Necesito que me ayudes con algo y te pido que no lo comentes con nadie por ahora.
8:07 a.m.

4 Voy entrando a consejo. Pásame tu celular y seguimos por WhatsApp.
8:08 a.m.

5 Una última cosa: necesito el archivo y que me confirmes tu usuario del módulo.
8:11 a.m.

1. **El nombre lo escribe el atacante.** Cualquiera con su propio Microsoft 365 puede escribirte, y poner el nombre que quiera.
2. **La etiqueta «Externo».** Pequeña y gris, y es la única pista que da la herramienta. El dominio es la otra.
3. **«No lo comentes».** No protege ninguna negociación: **desactiva tu verificación.** Que te pidan callar es la razón para contarlo.
4. **Te sacan del canal corporativo.** En WhatsApp no hay etiqueta, ni registro, ni administración.
5. **La petición llega al final.** Nunca en el primer mensaje: para entonces ya hay confianza, secreto y prisa.

UNA LLAMADA O UNA NOTA DE VOZ

Reconocer la voz ya no es verificar

Nota de voz · 0:12



«Necesito que me ayudes con algo urgente, estoy en reunión y no puedo hablar ahora.»

Aquí no hay nada que mirar.
Ese es justamente el problema.

1. **Clonar una voz cuesta unos dólares** y necesita segundos de audio público. Si la persona habla en radio o televisión, ese material ya está disponible.
2. **Urgencia más «no puedo hablar».** Es el patrón exacto: te mete prisa y te quita la posibilidad de confirmar en el momento.
3. **Cuelga y devuelve la llamada al número que ya tenías.** Nunca al que te acaban de dar. Y pacten una palabra clave de equipo, en persona.

ANTES DE PEGAR ALGO EN UNA INTELIGENCIA ARTIFICIAL

Lo que pegas deja de ser tuyo

Resúmeme este memorando y dime qué tengo que hacer.

MEM-NOM-2026-0417 · Uso interno
Patricia Londoño · C.C. 52.884.173 · Bancolombia 408-7719-4402
Andrés Cuéllar · C.C. 80.117.926 · Davivienda 0097-5531-8820

1. **Claro, aquí tienes el resumen en cinco puntos…**
2. Cuenta: personal · Historial: activado

1. **Salió del perímetro en el momento en que lo pegaste.** Está en un servidor de otra empresa, que también puede ser vulnerado. **Borrar el chat no lo trae de vuelta.**
2. **Con cuenta personal, la empresa no tiene ningún control.** Usa la corporativa, y desactiva el historial y el entrenamiento.
3. **Sin problema:** texto ya público, ideas generales, redacción sin datos. **Piénsalo:** documentos internos sin datos personales. **Nunca:** cédulas, contratos, nómina, claves, material no emitido, cifras no publicadas.

ANTES DE USAR UN DATO QUE TE DIO LA IA

No sabe que no sabe

¿Cuántas empresas colombianas reportaron incidentes de ciberseguridad en 2024?

1. Fueron **4.312 empresas**, un 23 % más que en 2023.
2. **Fuente:** Informe Nacional de Ciberseguridad, marzo de 2025, página 37.
3. — ¿Estás seguro de que ese informe existe?

Sí, es un informe público y verificable.

1. **Da la cifra con decimales y sin dudar.** No está construida para saber, sino para producir la continuación más plausible. Una mentira le sale igual de fluida que una verdad.
2. **Inventa la fuente con formato impecable.** Nombre, fecha y página. **Pídesela siempre y ábrela tú mismo.**
3. **No le preguntes a la IA si la IA tiene razón.** En el caso Mata contra Avianca el abogado lo hizo, le dijo que sí, y fue sancionado: las seis sentencias que citó no existían.

YA HICE CLIC · YA DI MIS DATOS

En este orden, y ya

1. **Reporta primero**, antes de intentar arreglarlo tú. Lo que decide el daño no es el clic: es cuánto tiempo pasa hasta el aviso.
2. **Cambia la contraseña** desde otro dispositivo, y en todos los sitios donde usaras la misma.
3. **Pide que cierren tus sesiones.** Con la sesión robada, el doble factor no frena nada, y cambiar la clave no la invalida.
4. **No borres nada.** El mensaje y la hora exacta son lo que permite medir el alcance.
5. **Avisa a quien pueda haber recibido lo mismo.** Casi nunca llega a una sola persona.

LA REGLA QUE LO DESARMA TODO

Nunca verifiques por el mismo canal por el que llegó la petición.

Si llegó por Teams, no lo confirmes por Teams. Llama al número que ya tenías, no al que te acaban de dar. Ninguna petición de dinero, claves o datos personales es válida solo por voz o por chat.

Dudar

Prisa, secreto o una excepción al procedimiento: esas tres cosas son la señal, no el contexto.

Verificar por otro canal

Nunca por donde llegó. Llama, camina, pregunta por otro lado.

Reportar

Aunque no estés seguro. Sobre todo si ya hiciste clic: las primeras horas lo son todo.