

Guía de bolsillo: antes del clic



Aprende. Prueba. Acuerda un paso.

01 Detente

La urgencia de un mensaje no demuestra que sea legítimo.

02 Verifica

Confirma solicitudes inusuales por un canal conocido, sin usar los enlaces del mensaje.

03 Reporta

Sigue el canal de seguridad de tu organización. Si ya interactuaste, avisa cuanto antes.

Una pregunta para conversar

Ejemplo ficticio: soporte@acceso-empresa.invalid te escribe: «Tu cuenta se cierra en 10 minutos. Entra al enlace y confirma tu contraseña». El mensaje tiene un logo impecable. ¿Qué haces antes de tocar el enlace?

Fuentes para ampliar (enlace activo): NIST: Phishing

Consulta: 10/09/2026 · Ejercicios propios. Ilustración editorial generada con IA.

Llévalo a tu equipo · Cursos 360

contacto@cursos360.cl | WhatsApp +56 9 9873 9673

cursos360.cl/contactanos/ · Las Condes, Santiago de Chile

De la idea al acuerdo.

10 minutos: exploren una situación (2), conecten con el trabajo (5) y acuerden una mejora (3). Usen ejemplos ficticios y datos generales.

¿Qué ya podemos confirmar?

- ☐ Sé a qué canal reportar un mensaje sospechoso.
- ☐ Verifico solicitudes inusuales por otra vía.
- ☐ Uso contraseñas únicas y autenticación multifactor cuando está disponible.
- ☐ Conozco qué hacer si abrí un enlace o compartí datos.

Una mejora que acordamos

Rol responsable y personas que deben participar

Fecha de revisión y cómo veremos si avanzamos

Para cerrar la conversación

¿Qué falta validar con la persona responsable? ¿Dónde quedará el acuerdo para poder revisarlo?

Llévalo a tu equipo · Cursos 360

contacto@cursos360.cl | WhatsApp +56 9 9873 9673

cursos360.cl/contactanos/ · Las Condes, Santiago de Chile