CIBERSEGURIDAD · RESPUESTA PRÁCTICA

Guía rápida antiphishing para equipos

Detén el clic, verifica por otro canal y reporta: una secuencia simple que reduce el riesgo.

Señales que merecen una pausa

[ ] Urgencia, amenaza o premio inesperado.	[ ] Remitente parecido al real, pero con cambios mínimos.
[ ] Solicitud de clave, código MFA, pago o datos sensibles.	[ ] Enlace acortado o dominio que no coincide.
[ ] Adjunto inesperado o formato poco habitual.	[ ] Mensaje que evita el proceso normal de aprobación.

Antes de hacer clic: VERIFICA

Paso	Qué hacer	Ejemplo
1. Pausa	No abras enlaces ni adjuntos. Lee el mensaje completo y separa urgencia de evidencia.	Una supuesta jefatura pide un pago en minutos.
2. Revisa	Comprueba dirección real, dominio, enlace y contexto. No confíes solo en nombre o logotipo.	Pasa el cursor sobre el enlace sin abrirlo.
3. Confirma	Usa un canal conocido e independiente: teléfono interno, chat corporativo o sitio escrito manualmente.	Llama a la persona usando el número del directorio.
4. Reporta	Envía el mensaje al canal de seguridad y conserva encabezados o captura si el procedimiento lo solicita.	Botón de reporte o mesa de ayuda.

Si ya hiciste clic

[ ] Desconecta el equipo de la red si el protocolo lo indica.	[ ] Informa de inmediato; no esperes a ver síntomas.
[ ] No borres el mensaje ni ocultes lo ocurrido.	[ ] Cambia credenciales desde un equipo seguro si te lo indican.
[ ] Revoca sesiones y activa controles con soporte TI.	[ ] Registra qué ingresaste, descargaste o autorizaste.

Regla de equipo: reportar rápido es una conducta de seguridad, no un motivo de castigo. La velocidad del aviso puede limitar el impacto.

Adapta esta guía al procedimiento de respuesta de tu organización. Referencia general: CSIRT de Gobierno de Chile. Revisión: septiembre de 2026.