tisec.cl

Ciberseguridad y cumplimiento para PYMEs chilenas

Guía Rápida Anti-Phishing

Tarjeta de referencia para empleados — Imprimir y conservar a mano

SEÑALES DE ALERTA EN UN CORREO

!	**Urgencia extrema**	"Tu cuenta se bloqueará en 24 horas." El objetivo es que no pienses antes de actuar.
!	**Remitente sospechoso**	El nombre dice "SII" pero el correo es sii-alertas@gmail.com. Siempre mira la dirección completa.
!	**Link que no coincide**	Pasa el mouse sobre el enlace SIN hacer clic. La URL real no coincide con el texto visible.
!	**Archivos adjuntos no solicitados**	Facturas o Word que no pediste. Nunca habilites macros si el archivo las solicita.
!	**Errores de redacción**	Frases extrañas, tildes que faltan, logos de baja calidad — señales de ataque automatizado.
!	**Solicitud de credenciales**	Ningún banco, el SII ni tu empresa pedirán tu contraseña por correo. Jamás.

SEÑUELOS MÁS COMUNES EN CHILE

- SII: "Notificación pendiente", "Declaración rechazada", "Fiscalización programada"
- Banco: "Movimiento sospechoso", "Su tarjeta fue bloqueada temporalmente"
- Correos de Chile / DHL: "Su paquete está retenido, pague el arancel"
- Microsoft / Google: "Su cuenta será desactivada, verifique ahora"
- CEO Fraud: Correo que parece de gerencia pidiendo transferencia urgente

QUÉ HACER SI SOSPECHAS

1. **NO hagas clic en ningún enlace ni descargues archivos adjuntos**
2. **NO respondas ni reenvíes el correo sospechoso**
3. **Repórtalo al equipo TI o responsable de seguridad de la empresa**
4. **Márcalo como spam/phishing en tu cliente de correo**
5. **Si ya hiciste clic: desconéctate de la red y avisa de inmediato a TI**

SI YA CAÍSTE — ACTÚA EN LOS PRÓXIMOS 10 MINUTOS

El tiempo es crítico. No te escondas — reportar rápido minimiza el daño.

1. **Desconecta el equipo de la red (Wi-Fi y cable) pero NO lo apagues**
2. **Cambia las contraseñas afectadas desde OTRO dispositivo limpio**
3. **Avisa a TI y a tu supervisor directamente (no por el equipo afectado)**
4. **Si entregaste datos bancarios: llama a tu banco en los próximos minutos**
5. **Documenta qué ocurrió: hora, correo recibido, qué hiciste, qué datos ingresaste**

Contacto de seguridad interno: _____ Tel: _____