Estimados/as funcionarios

En el marco de las medidas de seguridad realizadas por Departamento Tecnologías de la Información y Comunicaciones en periodo de alerta sanitaria y ante el aumento de ataques de phishing sucedidos en este periodo, se hace necesario reforzar medidas para protegernos de los fraudes vinculados a Covid-19, Bancarios, RRSS, etc. Al respecto se adjuntan recomendaciones para evitar ser víctima de estos ataques:

1. ¿Qué es el phishing?

El phishing es un ataque que se inicia enviando a la víctima una comunicación en la que, suplantando a una entidad conocida, le piden que haga clic en un enlace, descargue un fichero o envíe información sensible. Con el **objetivo de robar cuentas, contraseñas y otros datos, o infectar con malware[1].**

2. ¿Cómo protegerse el phishing?

- Mantener el **antivirus actualizado** y activado, con las firmas al día.
- Mantenerse atento a los ataques de ingeniería social. Si el mensaje insta a actuar rápidamente, es una oferta muy atractiva, adulan o amenazan, **¡Desconfíe!**
- No haga clic sobre una URL para introducir datos sin antes pasar el ratón sobre el enlace para comprobar si es legítimo el sitio hacia donde dirige.
- **Desconfíe de las URL** acortadas, pues no se puede comprobar si el destino es legítimo o no. Los sitios legales no las utilizan para solicitar datos.
- Antes de iniciar sesión en una web, comprueba su identidad: consulte los datos de certificado, en el candado de la barra de navegación. Verifique que usa **https://**.
- Antes de introducir el email, u otros datos sensibles, en una web o en un formulario lea y comprenda la política de privacidad y el aviso legal para evitar dar el consentimiento a que cedan esos datos a terceros y terminen en manos de ciberdelincuentes.
- Al descargar un archivo no haga clic en “habilitar contenido” saldo que confíe en la fuente de dónde procede. Si al descargar un fichero se solicitan permisos para habilitar contenido, no se fíe, podría iniciarse la descarga de malware.
- Ante cualquier sospecha, elimine el mensaje, cuelga la llamada o bloquee el contacto.

3. Creo que he sido víctima de phishing ¿qué debo hacer?

- Si piensas que has entregado información sensible de la organización de la que eres parte, reporta inmediatamente lo ocurrido a seguridadtic@minsal.cl y a tus jefaturas. Ellos deben alertar al resto de la organización de lo sucedido para que tomen precauciones.
- Si crees que has revelado información financiera y algunas cuentas pueden haber sido comprometidas, contacta rápidamente a tu banco o institución financiera y da orden de bloqueo de las cuentas que puedan estar en riesgo. Debes estar consciente que pueden ocurrir algunos cargos en dinero sobre tus cuentas producto de la estafa.

[1] Los **malwares** son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

- Cambia las contraseñas que pienses fueron reveladas. Si utilizas las mismas claves en diferentes cuentas, asegúrate de cambiar todas las cuentas y no reutilices esa contraseña en el futuro.
- Revisa entre todas tus cuentas, en tus programas y en tus dispositivos si existen señales que indiquen consecuencias de robo de información.
- Considera reportar el incidente a la Brigada de Cibercrimen de la PDI para que te puedan guiar sobre qué hacer en lo inmediato y para evitar que este tipo de incidentes vuelvan a ocurrir. En Santiago. F. 2 2708 0658 / Valparaíso. F. 32 226 1271 / Concepción F. 41 286 5130.

4. Recomendaciones Equipo respuesta CSIRT Ministerio Interior en estos temas

Se adjuntan las recomendaciones del Ministerio del Interior, para proteger sus datos en redes sociales, que también son aplicables a las credenciales en sitios institucionales.

- **Recomendaciones para proteger contraseñas en redes sociales**
- **Protocolos Ante Incidentes Spear Phishing**

5. Políticas de Seguridad

Finalmente les recordamos la importancia que conozcan las políticas de seguridad del Ministerio publicadas en intranet, disponibles en el siguiente enlace:

- **Políticas de Seguridad MINSAL**

Departamento Tecnologías de la Información y Comunicaciones