SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME ABRIL 2025

DE : **Matías Estay Esquivel**
Departamento de Informática
SECPLA

A : **Miguel Muñoz Verdugo**
Secretario Comunal de Planificación

Padre Hurtado, abril del 2025
En función del cometido descrito en antecedente, señalado:

1. **Enseñar practicas seguras de uso de internet y herramientas digitales para proteger la privacidad y seguridad de línea de los vecinos.**
2. **Colaborar en la creación y distribución de materiales educativos.**

A continuación, se presentan las acciones concretadas durante el periodo indicado, para los distintos cometidos asignados, perteneciente al programa de alfabetización digital:

1. **Enseñar practicas seguras de uso de internet y herramientas digitales para proteger la privacidad y seguridad de línea de los vecinos.**

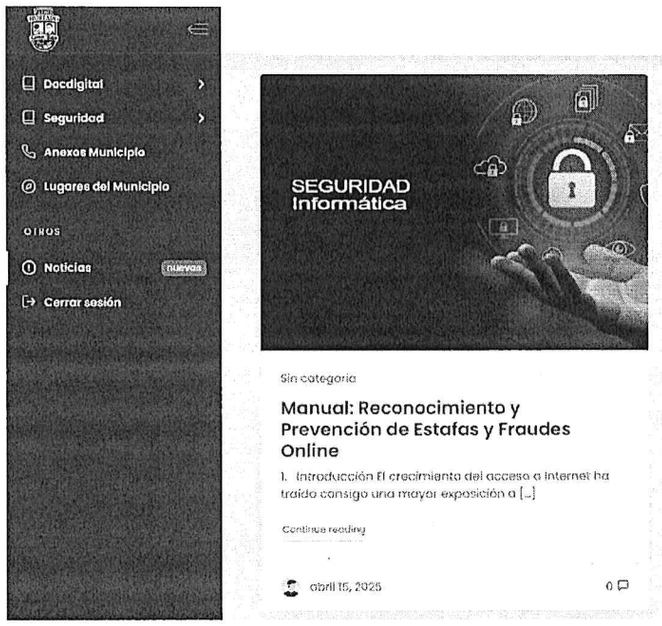
Durante este mes se elaboró un documento digital titulado:

"Reconocimiento y Prevención de Estafas y Fraudes Online".

Este material tiene como finalidad educar a la comunidad sobre cómo identificar correos electrónicos y mensajes fraudulentos, reconocer los métodos más comunes de estafas en línea (como phishing, suplantación de identidad, fraudes en redes sociales y soporte técnico falso), así como orientar sobre qué hacer en caso de ser víctima de una estafa.

El documento ha sido diseñado con un enfoque práctico y accesible, incluyendo ejemplos reales y consejos preventivos. Esta acción busca fortalecer el uso responsable y seguro de internet en la comunidad.

Importante: Este recurso se encuentra únicamente en formato digital, y ha sido compartido a través de la intranet municipal para facilitar su difusión y garantizar su disponibilidad continua como evidencia del trabajo realizado.



2. Colaborar en la creación y distribución de materiales educativos.

En línea con el compromiso de entregar herramientas educativas efectivas, se ha desarrollado el manual digital "Reconocimiento y Prevención de Estafas y Fraudes Online". Este documento forma parte del material oficial del programa de alfabetización digital, y fue trabajado para proporcionar contenido claro, estructurado y útil para cualquier vecino, independientemente de su nivel de conocimiento tecnológico.

Entre los temas destacados que aborda se encuentran:

- Cómo identificar correos sospechosos.
- Reconocimiento de intentos de phishing y suplantación de identidad.
- Medidas concretas para actuar frente a una estafa.
- Recomendaciones para crear contraseñas seguras y activar la autenticación de dos factores.

Este material fue distribuido únicamente en formato digital, lo cual permite mantener su actualización y facilitar el acceso remoto.Para garantizar su acceso a la comunidad, el manual ha sido distribuido en formato digital:

- **Versión digital**, disponible para descarga en la intranet de la municipalidad.

2. ¿Qué es una estafa o fraude online?

Una estafa online es un intento de engaño con el fin de obtener beneficios ilegítimos mediante medios digitales. Puede implicar la obtención de información personal, datos bancarios, contraseñas o incluso dinero, a través de engaños diseñados para parecer legítimos.

3. Cómo identificar correos electrónicos y mensajes fraudulentos

3.1 Señales comunes en correos sospechosos

- **Remitente desconocido o sospechoso**: direcciones de correo no oficiales.
- **Errores ortográficos o gramaticales**: suelen ser indicios de estafas
- **Urgencia o amenazas**: mensajes como "¡Tu cuenta será cerrada en 24 horas!"
- **Solicitan información personal**: ningún banco o empresa legítima pide datos sensibles por correo.
- **Enlaces falsos**: enlaces que parecen correctos, pero llevan a sitios peligrosos.
- **Archivos adjuntos sospechosos**: pueden contener malware.

3.2 Ejemplo de phishing real

Asunto: "Notificación urgente de seguridad bancaria"
Mensaje: "Detectamos una actividad inusual en su cuenta. Inicie sesión aquí para verificar su información."
Enlace: https://banco-seguro-clientes.xyz (parece real, pero es fraudulento)

4. Métodos comunes de estafa en línea

4.1 Phishing

4.2 Suplantación de identidad

Los estafadores se hacen pasar por amigos, familiares o empresas conocidas para engañar.
Ejemplo: mensaje de WhatsApp diciendo "Hola mamá, cambié de número".

4.3 Estafas en redes sociales

Cuentas falsas que ofrecen premios, becas o ayudas a cambio de datos.
Ejemplo: sorteos falsos de celulares o notebooks.

4.4 Estafas de soporte técnico

Recibes llamadas o mensajes diciendo que tu equipo está infectado. Piden acceso remoto y terminan robando información.

4.5 Estafas en compras online

Tiendas falsas que desaparecen tras recibir el dinero.
Ejemplo: páginas en Instagram con productos a precios exageradamente bajos.

5. Qué hacer si eres víctima de una estafa

1) No entres en pánico.
2) Cambia todas tus contraseñas
3) Contacta a tu banco si compartiste información financiera.
4) Revisa tus dispositivos con antivirus actualizado
5) Guarda toda la evidencia (capturas, correos, nombres de usuario)
6) Denuncia el hecho en:
7) En Chile: www.pdi.cl o www.ciberseguridad.gob.cl
8) En otros países: policía cibernética o CERT correspondiente.
9) Informa a tus contactos si tu cuenta fue comprometida.

6. Consejos prácticos para protegerte

- Usa **contraseñas seguras** y diferentes para cada servicio.
- Activa la **verificación en dos pasos**.
- Nunca hagas clic en enlaces sospechosos.
- Mantén tu sistema operativo y antivirus actualizados.
- Revisa siempre la URL del sitio donde ingresas tus datos.
- Desconfía de ofertas "demasiado buenas para ser verdad".

7. Recursos y contactos útiles

- Centro Nacional de Ciberseguridad (Chile): https://www.ciberseguridad.gob.cl
- Policía de Investigaciones (PDI): https://www.pdichile.cl
- CERT (Computer Emergency Response Team) de tu país
- Google Seguridad: https://safety.google
- Microsoft Protección: https://support.microsoft.com/security

8. Conclusión

La mejor herramienta contra el fraude es la **educación**. Hoy más que nunca, debemos ser conscientes de los riesgos online y actuar con responsabilidad. Identificar una estafa puede ahorrarnos muchos problemas. Este manual pretende ser una guía clara y útil para que cualquier persona, sin importar su nivel técnico, pueda navegar de forma más segura.

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Sin otro particular, se despide atentamente,

[redacted]