SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME OCTUBRE 2026

DE : Diego Ignacio Marín Farías
Departamento de Informática
SECPLA

A : Miguel Muñoz Verdugo
Secretario Comunal de Planificación

Padre Hurtado, octubre del 2026

En función del cometido descrito en antecedente, señalado:

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

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

- **Concientización en el marco del Mes de la Ciberseguridad:**

  En el contexto del Mes de la Ciberseguridad, se informó y sensibilizó a la comunidad respecto de los fraudes digitales más frecuentes, en los que ciberdelincuentes se hacen pasar por bancos, empresas de servicios, tiendas o instituciones públicas con el fin de obtener claves y datos personales.

  Se explicaron las principales modalidades de engaño: el phishing (correos electrónicos falsos), el smishing (mensajes de texto falsos) y el vishing (llamadas telefónicas fraudulentas), destacando que la mayoría de estas estafas comienzan con un mensaje que aparenta ser oficial.
- **Identificación de señales de alerta:**
  Se enseñó a la comunidad a reconocer las características de los mensajes y llamadas que pueden corresponder a un intento de fraude, tales como:

  A. Avisos de cuentas bloqueadas, deudas, multas o premios pendientes.
  B. Solicitudes urgentes de claves, códigos recibidos en el celular o datos de tarjetas.
  C. Enlaces acortados o direcciones web parecidas, pero no iguales, a las oficiales.
  D. Remitentes desconocidos, errores de ortografía o saludos genéricos.
  E. Peticiones para instalar aplicaciones con el pretexto de "ayudar" o "proteger la cuenta".

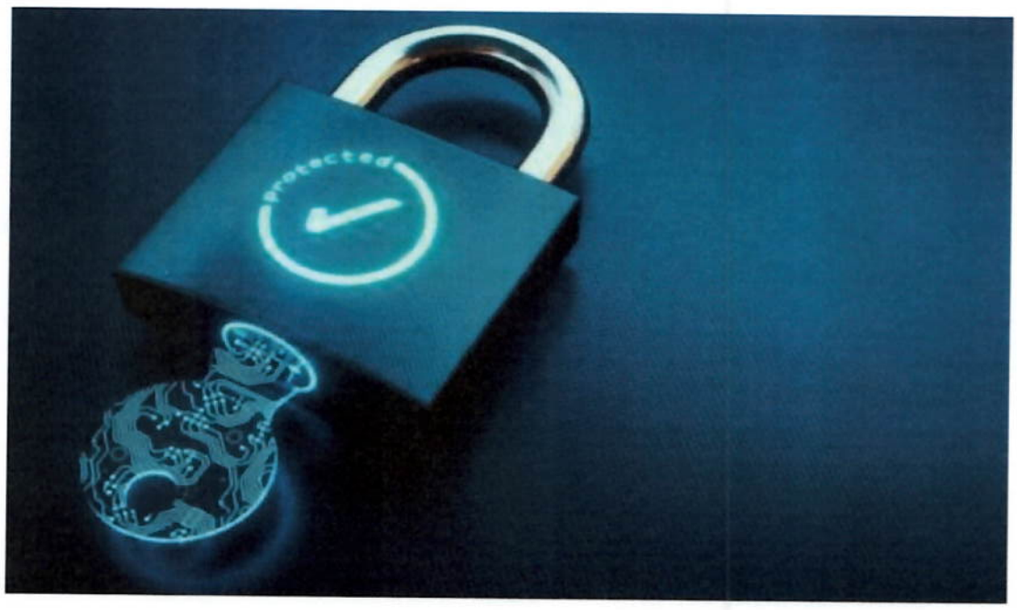
- **Promoción de buenas prácticas para protegerse de fraudes digitales:**
  Se difundieron recomendaciones preventivas destinadas a evitar la entrega de información personal y financiera a terceros, entre las que destacan:

  A. No hacer clic en enlaces de mensajes inesperados e ingresar escribiendo directamente la dirección del sitio oficial.
  B. Ante una llamada del banco, cortar y llamar al número que aparece en el reverso de la tarjeta.
  C. No compartir claves, códigos de verificación ni coordenadas, aunque se indique que es para un trámite.
  D. Tomarse el tiempo necesario antes de actuar, ya que la urgencia es la principal herramienta de los estafadores.
  E. En caso de haber sido víctima de un engaño, bloquear las tarjetas llamando al banco y cambiar las contraseñas.

- **Promoción de una cultura de prevención digital:**

  Se reforzó que ningún banco, empresa ni institución pública solicitará por teléfono, correo o mensaje las claves, el código que llega al celular ni los datos de la tarjeta o tarjeta de coordenadas.

Se destacó que cada persona cumple un rol relevante en la prevención de fraudes, deteniéndose a verificar antes de responder y compartiendo estas recomendaciones con su entorno.



Seguridad informática

Octubre, Mes de la Ciberseguridad: aprende a reconocer los fraudes digitales

En la Municipalidad de Padre Hurtado nos sumamos al Mes de la Ciberseguridad y queremos [...]

Continue reading

2. Colaborar en la creación y distribución de materiales educativos

- **Elaboración de contenido preventivo:**
  Se redactó y estructuró el material de difusión digital titulado **"OCTUBRE, MES DE LA CIBERSEGURIDAD: APRENDE A RECONOCER LOS FRAUDES DIGITALES"**, diseñado para entregar información clara y accesible sobre los engaños más comunes que circulan por correo electrónico, mensajes de texto y llamadas telefónicas.

  El material fue elaborado con un enfoque preventivo, orientado a que los vecinos y vecinas reconozcan las señales de alerta y eviten entregar sus claves, códigos de verificación y datos personales o financieros.

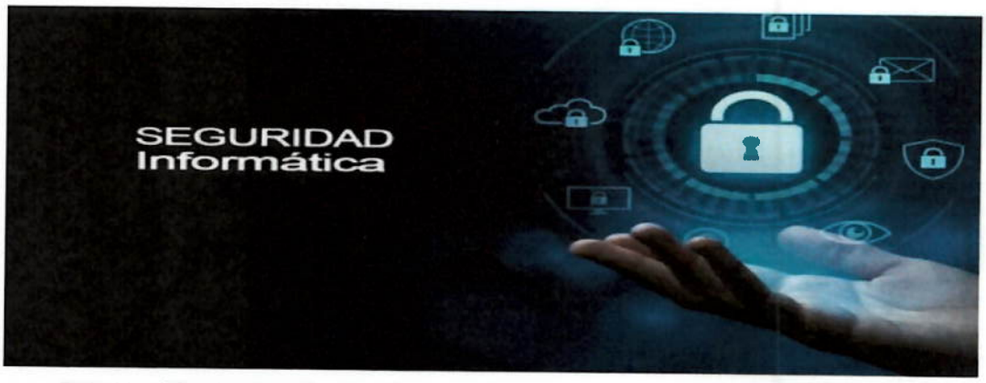
- **Elaboración de contenido visual e informativo:**
  El material incluyó recursos didácticos destinados a facilitar la comprensión de los principales riesgos y medidas preventivas:

  A. **Modalidades de fraude:** Se explicaron el phishing, el smishing y el vishing, y cómo los ciberdelincuentes suplantan a bancos, empresas e instituciones públicas.
  B. **Señales de alerta:** Se presentaron ejemplos de mensajes sobre cuentas bloqueadas, deudas o premios, solicitudes urgentes de claves, enlaces sospechosos y remitentes desconocidos.
  C. **Buenas prácticas:** Se entregaron recomendaciones para ingresar directamente a los sitios oficiales, devolver las llamadas al número oficial del banco, no compartir códigos y actuar con calma.
  D. **Ejemplos comparativos:** Se presentó un contraste entre una conducta de riesgo (hacer clic en un SMS que anuncia el bloqueo de la cuenta) y una conducta segura (ignorar el enlace y revisar la cuenta desde la aplicación oficial del banco).
  E. **Regla de Oro:** Se incorporó un apartado destacado recordando que ningún banco, empresa ni institución pública solicitará por teléfono, correo o mensaje las claves, el código que llega al celular ni los datos de la tarjeta.

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

- **Difusión del material:**

El contenido fue preparado para su publicación y distribución a través de los canales digitales institucionales, particularmente la intranet municipal, con el objetivo de facilitar el acceso de vecinos, vecinas, funcionarios y colaboradores a recomendaciones para reconocer y prevenir fraudes digitales en el marco del Mes de la Ciberseguridad.



En la Municipalidad de Padre Hurtado nos sumamos al Mes de la Ciberseguridad y queremos ayudarte a reconocer los engaños más comunes que circulan por correo, mensajes de texto y llamadas telefónicas.

¿SABÍAS QUE LA MAYORÍA DE LAS ESTAFAS DIGITALES COMIENZAN CON UN MENSAJE QUE PARECE OFICIAL?

Los ciberdelincuentes se hacen pasar por bancos, empresas de servicios, tiendas o instituciones públicas para que entregues tus claves o datos personales. Estas técnicas se conocen como phishing (correos falsos), smishing (SMS falsos) y vishing (llamadas fraudulentas).

SEÑALES DE ALERTA MÁS COMUNES

Desconfía si recibes un mensaje o llamada que:

- Te avisa que tu cuenta fue bloqueada o que tienes una deuda, multa o premio pendiente
- Te pide con urgencia tu clave, el código que llegó a tu celular o los datos de tu tarjeta
- Incluye un enlace acortado o una dirección web parecida, pero no igual, a la oficial
- Viene de un remitente desconocido, tiene errores de ortografía o un saludo genérico
- Te pide instalar una aplicación para "ayudarte" o "proteger tu cuenta"

¿CÓMO PROTEGERTE?

- No hagas clic en enlaces de mensajes inesperados: ingresa escribiendo tú mismo la dirección del sitio oficial
- Si te llaman de tu banco, corta y llama tú al número que aparece en el reverso de tu tarjeta
- Nunca compartas claves, códigos de verificación ni coordenadas, aunque te digan que es para un trámite
- Tómate tu tiempo: la urgencia es la principal herramienta de los estafadores
- Si caíste en un engaño, bloquea tus tarjetas de inmediato llamando a tu banco y cambia tus contraseñas

Ejemplo:

✗ Hacer clic en un SMS que dice "Su cuenta será bloqueada hoy, actualice sus datos aquí"

✓ Ignorar el enlace y revisar tu cuenta ingresando directamente a la app oficial del banco

REGLA DE ORO

Sin otro particular, se despide atentamente,

Miguel Muñoz Verdugo
Director SECPLA
Municipalidad de Padre Hurtado

Diego Ignacio Marín Farías
Departamento de Informática