SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME MAYO 2026

DE : **Alexis Antonio Alegría Riveros**
Unidad de Informática
SECPLA

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

Padre Hurtado, mayo del 2026
En función del cometido descrito en antecedente, señalado:

- **Crear materiales educativos adaptadas a las necesidades de los vecinos, incluyendo guías, manuales y tutoriales.**
- **Desarrollar campañas de sensibilización sobre ciberseguridad.**

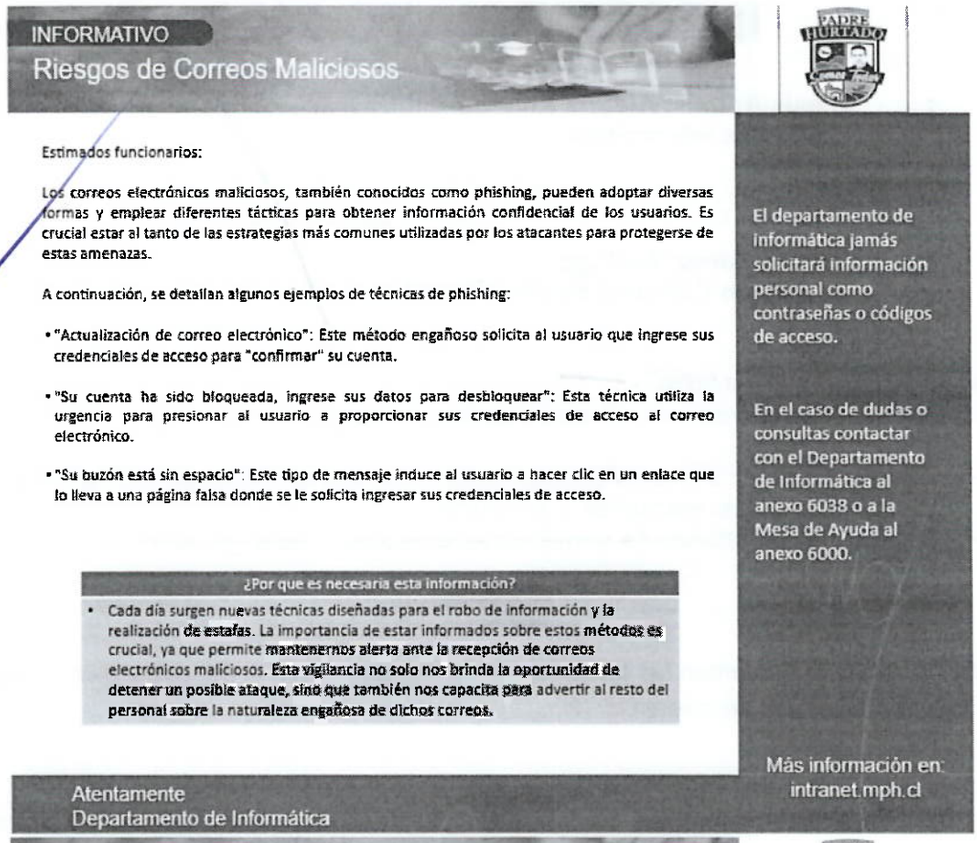
A continuación, se presentan las acciones concretadas durante el periodo indicado, para las distintas iniciativas de inversión:

Se compartieron diferentes comunicados por medio de correo electrónico con el fin de que los funcionarios se mantengan informados e informen a los vecinos de Padre Hurtado sobre los delitos cibernéticos más comunes (Anexo 1).

Se habilitó un espacio en la Intranet destinada a los funcionarios municipales donde pueden encontrar material relacionado al área tecnológica y el uso de algunas herramientas TIC de uso diario (Anexo 2).

ANEXOS

Anexo 1



INFORMATIVO

Riesgos de Correos Maliciosos

Estimados funcionarios:

Los correos electrónicos maliciosos, también conocidos como phishing, pueden adoptar diversas formas y emplear diferentes tácticas para obtener información confidencial de los usuarios. Es crucial estar al tanto de las estrategias más comunes utilizadas por los atacantes para protegerse de estas amenazas.

A continuación, se detallan algunos ejemplos de técnicas de phishing:

- "Actualización de correo electrónico": Este método engañoso solicita al usuario que ingrese sus credenciales de acceso para "confirmar" su cuenta.
- "Su cuenta ha sido bloqueada, ingrese sus datos para desbloquear": Esta técnica utiliza la urgencia para presionar al usuario a proporcionar sus credenciales de acceso al correo electrónico.
- "Su buzón está sin espacio": Este tipo de mensaje induce al usuario a hacer clic en un enlace que lo lleva a una página falsa donde se le solicita ingresar sus credenciales de acceso.

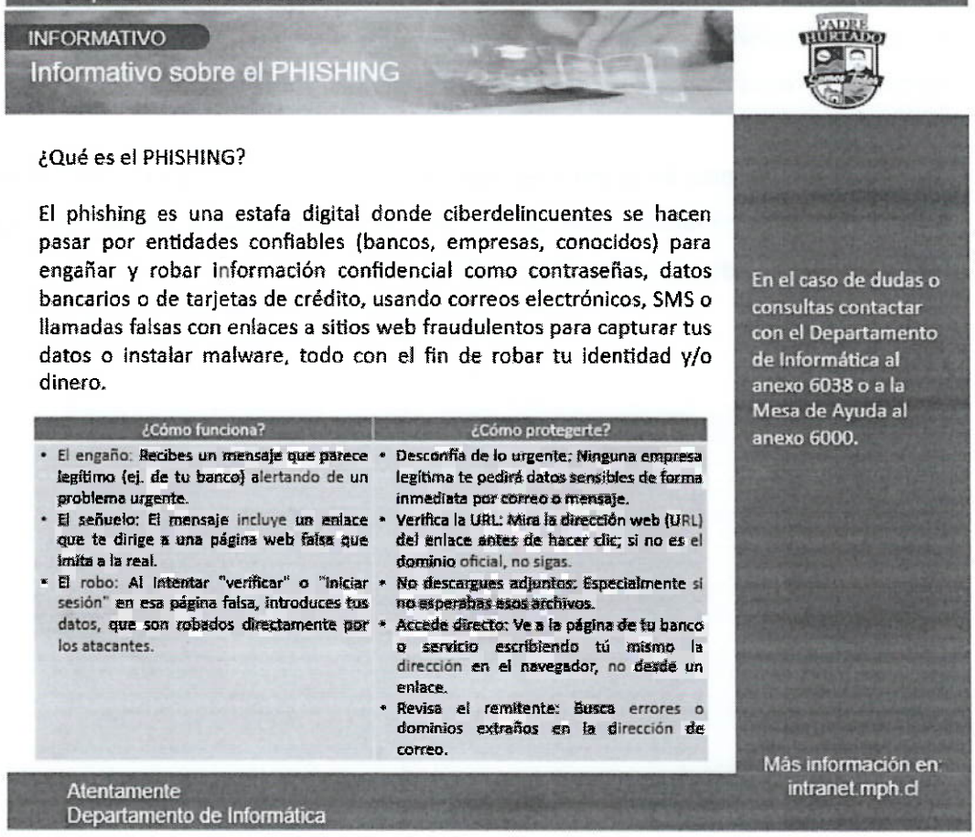
¿Por qué es necesaria esta información?
• Cada día surgen nuevas técnicas diseñadas para el robo de información y la realización de estafas. La importancia de estar informados sobre estos métodos es crucial, ya que permite mantenernos alerta ante la recepción de correos electrónicos maliciosos. Esta vigilancia no solo nos brinda la oportunidad de detener un posible ataque, sino que también nos capacita para advertir al resto del personal sobre la naturaleza engañosa de dichos correos.

El departamento de informática jamás solicitará información personal como contraseñas o códigos de acceso.

En el caso de dudas o consultas contactar con el Departamento de Informática al anexo 6038 o a la Mesa de Ayuda al anexo 6000.

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática



INFORMATIVO

Informativo sobre el PHISHING

¿Qué es el PHISHING?

El phishing es una estafa digital donde ciberdelincuentes se hacen pasar por entidades confiables (bancos, empresas, conocidos) para engañar y robar información confidencial como contraseñas, datos bancarios o de tarjetas de crédito, usando correos electrónicos, SMS o llamadas falsas con enlaces a sitios web fraudulentos para capturar tus datos o instalar malware, todo con el fin de robar tu identidad y/o dinero.

¿Cómo funciona?	¿Cómo protegerte?
• El engaño: Recibes un mensaje que parece legítimo (ej. de tu banco) alertando de un problema urgente. • El señuelo: El mensaje incluye un enlace que te dirige a una página web falsa que imita a la real. • El robo: Al intentar "verificar" o "iniciar sesión" en esa página falsa, introduces tus datos, que son robados directamente por los atacantes.	• Desconfía de lo urgente: Ninguna empresa legítima te pedirá datos sensibles de forma inmediata por correo o mensaje. • Verifica la URL: Mira la dirección web (URL) del enlace antes de hacer clic; si no es el dominio oficial, no sigas. • No descargues adjuntos: Especialmente si no esperabas esos archivos. • Accede directo: Ve a la página de tu banco o servicio escribiendo tú mismo la dirección en el navegador, no desde un enlace. • Revisa el remitente: Busca errores o dominios extraños en la dirección de correo.

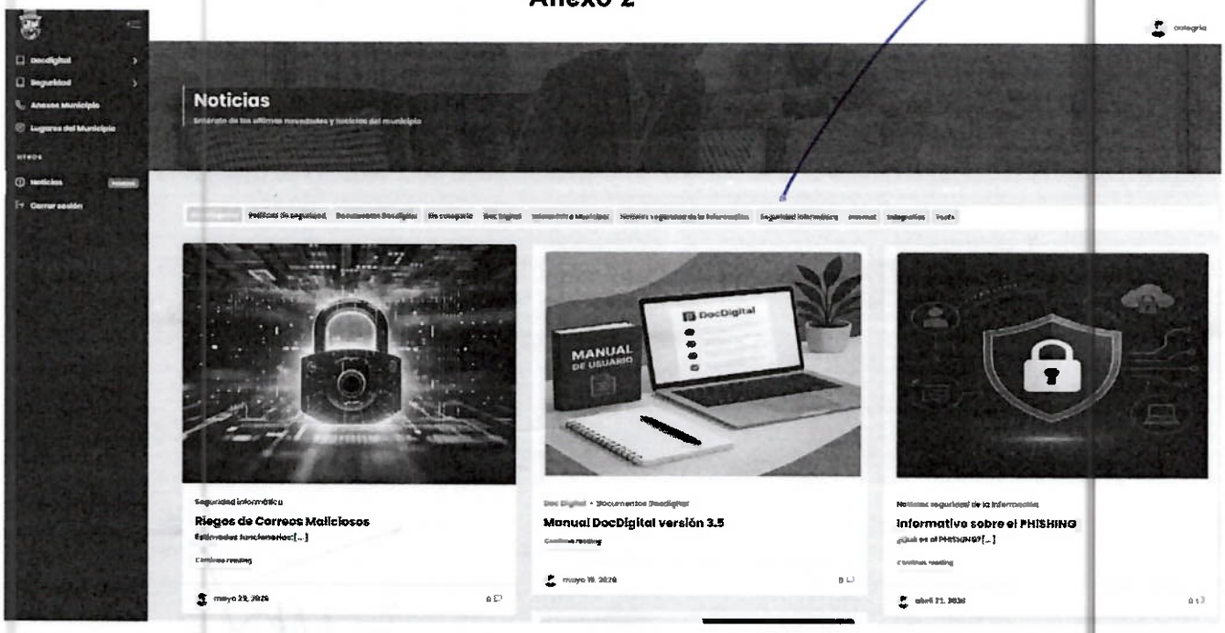
En el caso de dudas o consultas contactar con el Departamento de Informática al anexo 6038 o a la Mesa de Ayuda al anexo 6000.

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Anexo 2



Sin otro particular, se despide atentamente,

[redacted]