¿Qué es el Phishing?

El phishing es una técnica de ciberataque que busca engañar a las personas para que revelen información confidencial como:

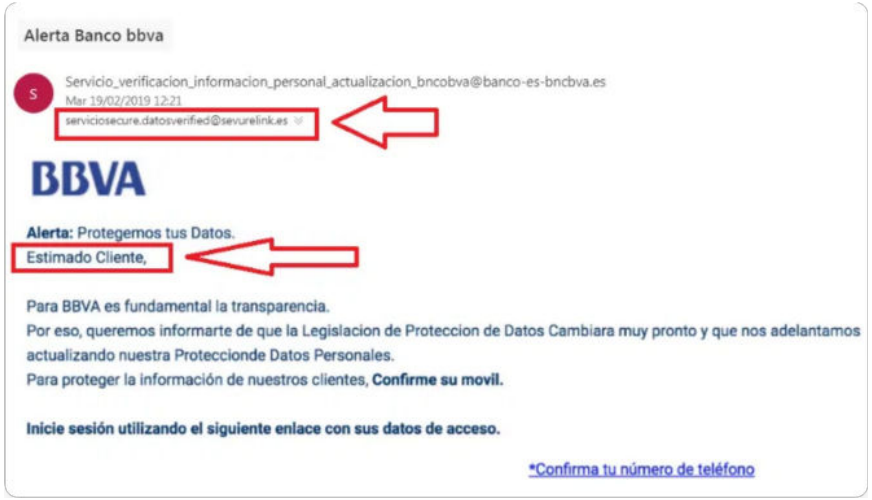
- Contraseñas y credenciales de acceso
- Datos bancarios y financieros
- Información personal y laboral

¿Cómo funciona?

Los atacantes se hacen pasar por entidades o personas de confianza (bancos, servicios públicos, compañeros de trabajo) para engañar a las víctimas y lograr que realicen acciones como:

- Hacer clic en enlaces maliciosos
- Descargar archivos infectados
- Proporcionar información confidencial

Como Municipalidad de Melipilla, proteger la información es responsabilidad de todos. El phishing puede comprometer datos sensibles de los funcionarios, ciudadanos y la operación municipal.



Tipos comunes de Phishing

Phishing por correo electrónico

El más común. Correos que suplantan entidades legítimas como bancos, servicios públicos o plataformas conocidas.

Smishing (SMS)

Mensajes de texto que contienen enlaces maliciosos o solicitan información personal, a menudo simulando ser notificaciones oficiales.

Vishing (llamadas)

Llamadas telefónicas donde el atacante se hace pasar por una entidad oficial para obtener información confidencial.

Spear Phishing

Ataques dirigidos y personalizados que utilizan información específica sobre la víctima para parecer más creíbles.

Pharming

Redirige el tráfico de un sitio web legítimo a uno falso, sin que el usuario se dé cuenta del cambio.

I. MUNICIPALIDAD MELIPILLA

Señales de alerta en correos de Phishing

I. MUNICIPALIDAD MELIPILLA

Errores ortográficos y gramaticales

Los correos fraudulentos suelen contener errores de escritura, mala gramática o redacción extraña.

Remitente sospechoso

Direcciones de correo que imitan a entidades legítimas pero con pequeñas variaciones o dominios extraños.

Solicitud de información personal

Peticiones urgentes de datos personales, contraseñas o información financiera.

Enlaces sospechosos

URLs que parecen legítimas pero con pequeñas diferencias. Al pasar el cursor sobre ellas, muestran direcciones diferentes.

Sentido de urgencia

Mensajes que presionan para actuar rápidamente, amenazando con consecuencias si no se responde de inmediato.

Ejemplos reales de Phishing

I. MUNICIPALIDAD MELIPILLA

Suplantación de entidades bancarias

Correos que simulan ser de bancos solicitando "verificar" información de la cuenta o alertando sobre problemas de seguridad.

- URLs falsas
- Logos mal replicados
- Solicitud de datos

Suplantación de servicios municipales

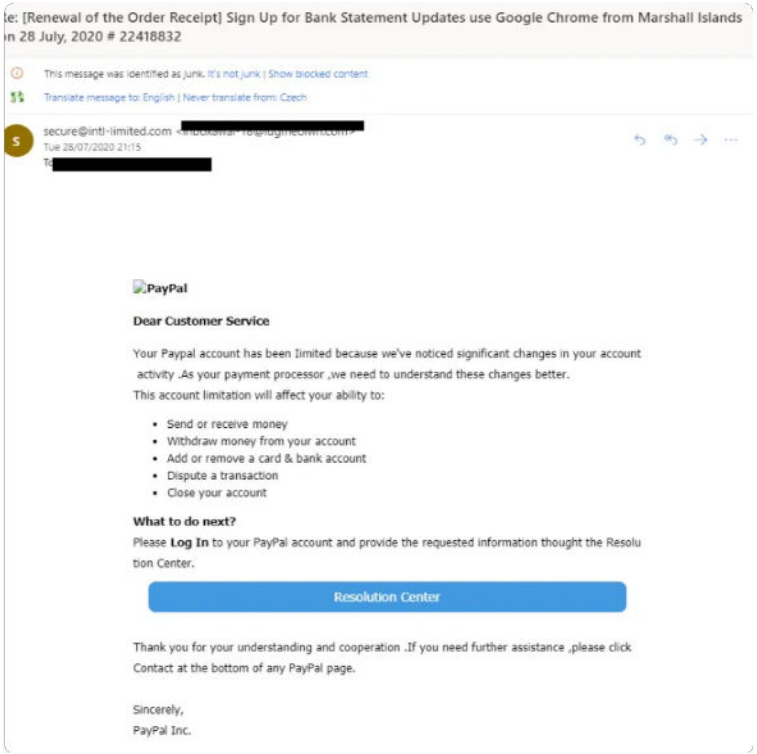
Correos que simulan ser de la municipalidad solicitando actualización de datos o pago de servicios a través de enlaces fraudulentos.

- Dominio incorrecto
- Errores gramaticales
- Urgencia injustificada

Correos de "premios" o "herencias"

Mensajes que informan sobre supuestos premios o herencias inesperadas que requieren datos personales para el cobro.

- Ofertas irreales
- Remitente desconocido
- Solicitud de pago anticipado



e: [Renewal of the Order Receipt] Sign Up for Bank Statement Updates use Google Chrome from Marshall Islands
n 28 July, 2020 # 22418832

This message was identified as junk. It's not junk | Show blocked content

Translate message to: English | Never translate from: Czech

secure@intl-limited.com [redacted]
Tue 28/07/2020 21:15
[redacted]

PayPal

Dear Customer Service

Your Paypal account has been limited because we've noticed significant changes in your account activity .As your payment processor ,we need to understand these changes better.
This account limitation will affect your ability to:

- Send or receive money
- Withdraw money from your account
- Add or remove a card & bank account
- Dispute a transaction
- Close your account

What to do next?

Please **Log In** to your PayPal account and provide the requested information thought the Resolution Center.

Resolution Center

Thank you for your understanding and cooperation .If you need further assistance ,please click Contact at the bottom of any PayPal page.

Sincerely,
PayPal Inc.

Análisis de los ejemplos recibidos

I. MUNICIPALIDAD MELIPILLA

Suplantación de entidad bancaria

- Señales numeradas que indican elementos sospechosos en el correo
- Uso de logos oficiales para dar apariencia de legitimidad
- Enlaces que redirigen a sitios fraudulentos

Mensajes de oficina de correos

- Remitente desconocido que no corresponde a una entidad oficial
- Solicita hacer clic en un enlace sospechoso
- El enlace no utiliza HTTPS, indicando falta de seguridad

Mejores prácticas para prevenir el Phishing

I. MUNICIPALIDAD MELIPILLA

Verificar siempre el remitente

Comprobar cuidadosamente la dirección de correo electrónico del remitente, no solo el nombre mostrado.

Revisar los enlaces antes de hacer clic

Pasar el cursor sobre los enlaces para ver la URL real y verificar que corresponda a sitios oficiales.

No compartir información sensible por correo

Las entidades legítimas nunca solicitan contraseñas, datos bancarios o información personal por correo electrónico.

Mantener actualizado el software

Actualizar regularmente el sistema operativo, navegadores y antivirus para protegerse contra vulnerabilidades conocidas.

Reportar correos sospechosos

Informar inmediatamente al departamento de Informática de la Municipalidad sobre cualquier correo sospechoso recibido.

¿Qué hacer si sospecha de Phishing?

I. MUNICIPALIDAD MELIPILLA

1 No interactúe con el correo

No haga clic en enlaces, no descargue archivos adjuntos y no responda al mensaje sospechoso.

2 Reporte inmediatamente

Notifique al departamento de TI de la Municipalidad enviando el correo sospechoso a **informatica@munimelipilla.cl**

3 Si ya interactuó con el correo

Cambie inmediatamente sus contraseñas desde un dispositivo seguro y notifique a informatica@munimelipilla.cl

4 Verifique por canales oficiales

Si recibe una comunicación sospechosa, contacte a la organización a través de sus canales oficiales.

⚠ ¡Importante!

La rapidez en la respuesta es crucial para minimizar riesgos para la Municipalidad.

Resumen y conclusiones

I. MUNICIPALIDAD MELIPILLA

- El phishing es una técnica de ciberataque que busca engañar a las personas para obtener información confidencial mediante suplantación de identidad.
- Existen diversos tipos: correo electrónico, SMS (smishing), llamadas (vishing), dirigido (spear phishing), entre otros.
- Las señales de alerta incluyen: errores ortográficos, remitentes sospechosos, solicitudes urgentes de información y enlaces extraños.
- Ante un posible phishing: no interactuar, reportar inmediatamente, cambiar contraseñas si es necesario y verificar por canales oficiales.

Conclusión

La seguridad de la información en la Municipalidad de Melipilla es responsabilidad de todos. Mantenerse alerta y seguir las mejores prácticas de seguridad nos protege a todos y salvaguarda los datos de nuestros funcionarios y ciudadanos.