WILCOMP

S.A.S.

Phishing (Identificar y evitar fraudes)

---

a. Contenido

- **Definición de phishing y ejemplos comunes.**
- **Cómo identificar correos electrónicos fraudulentos.**
- **Verificación de enlaces sin hacer clic.**
- **Reconocimiento de sitios web falsos.**
- **Procedimiento para reportar intentos de phishing.**
- **Buenas prácticas para proteger contraseñas y datos bancarios.**

---

b. Introducción

El phishing es una técnica de ciberdelincuencia en la que los atacantes se hacen pasar por empresas legítimas (bancos, Netflix, Microsoft, Amazon, etc.) con el objetivo de engañarlo para que revele sus contraseñas, números de tarjeta de crédito u otra información confidencial.

Estos ataques suelen llegar por correo electrónico, mensajes de texto (SMS) o incluso llamadas telefónicas. Los mensajes crean una sensación de urgencia ("su cuenta será cerrada", "su paquete no puede ser entregado") para que usted actúe sin pensar. Este tutorial le enseñará a reconocer estas estafas y a protegerse sin necesidad de herramientas técnicas avanzadas.

---

c. Paso a Paso

1. Reconocer señales de alerta en correos electrónicos

Cuando reciba un correo inesperado que solicite información personal o haga clic en un enlace, verifique los siguientes puntos:

Señal de alerta	Ejemplo
Remitente sospechoso	El nombre muestra “Banco Nacional” pero la dirección real es banco-seguro@hotmail.com en lugar de @bancnacional.com.
Saludo genérico	“Estimado cliente” en lugar de su nombre completo.
Urgencia o amenaza	“Su cuenta será suspendida en 24 horas si no verifica sus datos”.
Errores ortográficos o gramaticales	“Por favor, verifique su cuentra” (con “cuentra” en lugar de “cuenta”).
Enlaces que no coinciden	El texto del enlace dice “www.mibanco.com” pero al pasar el mouse se ve u dirección diferente.
Solicitud de datos personales	Un banco nunca le pedirá su contraseña o número de tarjeta por correo.

2. Verificar enlaces sin hacer clic

Esta es una de las técnicas más importantes. Antes de hacer clic en cualquier enlace dentro de un correo:

1. **Coloque el mouse sobre el enlace (no haga clic).**
2. **Observe la esquina inferior izquierda de su navegador o la ventana del correo. Allí aparecerá la dirección web real.**
3. **Compare con la dirección oficial de la empresa:**
    - **Dirección falsa: http://banco-seguro.xyz/verificar**
    - **Dirección verdadera: https://www.bancooficial.com**
4. **Si la dirección no coincide o parece extraña (dominios como .xyz, .top, números en lugar de letras), no haga clic.**

3. Reconocer sitios web falsos

Si accidentalmente hizo clic en un enlace, preste atención a la página que se abre:

- **Verifique la barra de direcciones: debe tener un candado (🔒) y la dirección debe coincidir exactamente con la empresa. Los sitios falsos suelen tener direcciones como https://banco-oficial.secure-login.com en lugar de https://bancooficial.com.**
- **Observe la calidad visual: los sitios falsos pueden tener logotipos mal recortados, colores incorrectos o formularios que piden datos que la empresa real nunca solicitaría (contraseña + número de tarjeta al mismo tiempo).**
- **Pruebe con un dato falso: si la página le pide iniciar sesión, escriba un usuario y contraseña inventados. Si la página "acepta" datos falsos, es claramente fraudulenta.**

4. Qué hacer si sospecha que es phishing

1. **No haga clic en ningún enlace ni descargue archivos adjuntos.**
2. **No responda al correo. Al responder, confirma al atacante que su dirección de correo es válida.**
3. **Marque el correo como phishing:**
    - **En Gmail: Abra el correo, haga clic en los tres puntos verticales (⋮) y seleccione "Denunciar phishing".**
    - **En Outlook: Seleccione el correo, vaya a la barra superior y elija "Correo no deseado" > "Phishing".**
4. **Si ingresó datos en un sitio falso:**
    - **Cambie inmediatamente su contraseña desde el sitio oficial (escribiendo la dirección manualmente en el navegador, no desde el enlace del correo).**
    - **Si entregó datos bancarios, contacte a su banco de inmediato.**
    - **Active la autenticación de dos factores (2FA) en sus cuentas importantes.**

5. Buenas prácticas para evitar phishing

- **Acceda a sitios sensibles escribiendo la dirección manualmente: nunca haga clic en enlaces de correos para entrar a su banco, PayPal, Amazon, etc.**
- **Active la autenticación de dos factores (2FA): aunque roben su contraseña, no podrán acceder sin el código de su teléfono.**

- **Mantenga actualizado su navegador: los navegadores modernos (Edge, Chrome, Firefox) tienen protección contra sitios de phishing.**
- **Desconfíe de ofertas demasiado buenas: "Ganó un iPhone", "Premio de lotería", etc., son casi siempre estafas.**
- **No comparta contraseñas por ningún medio: ninguna empresa legítima le pedirá su contraseña por teléfono, correo o mensaje de texto.**

---

d. Conclusión

El phishing es una amenaza constante, pero completamente evitable con hábitos simples. La regla de oro es: Nunca entregue información personal después de hacer clic en un enlace recibido por correo o mensaje. Siempre verifique la fuente.

Resumen de acciones clave:

1. **Verifique siempre la dirección del remitente y los enlaces antes de hacer clic.**
2. **Ante la duda, acceda manualmente al sitio oficial escribiendo la URL.**
3. **Reporte los correos sospechosos para ayudar a proteger a otros usuarios.**
4. **Si cayó en un engaño, actúe rápido: cambie contraseñas y contacte a su banco.**

La seguridad en Internet depende en gran medida de la atención y la prudencia. Con estas herramientas, usted puede navegar con mayor confianza y proteger su información personal.