

Clase: Prevención de Phishing en el Entorno Empresarial

Objetivo:

Capacitar al personal de la empresa para reconocer, evitar y reportar intentos de phishing, protegiendo tanto la información personal como la de la organización.

1. ¿Qué es el Phishing?

Es un ciberataque en el que un atacante se hace pasar por una entidad confiable para robar:

- Contraseñas
- Datos bancarios
- Información confidencial



Tu cuenta ha sido suspendida.
Haz clic aquí para verificar tu identidad.



Es un ciberataque en el que un atacante se hace pasar por una entidad confiable para robar:

- Contraseñas
- Datos bancarios
- Información confidencial

Ejemplo: "Tu cuenta ha sido suspendida. Haz clic aquí para verificar tu identidad."

2. Tipos Comunes de Phishing

EMAIL PHISHING

Descripción

Correos falsos que aparentan ser de bancos o jefes.

**Factura
pendiente,
abre el PDF**





Hola, Juan!

**Tu cuenta ha sido
suspendida**

Haz clic aquí para verificar tu cuenta



Maria Gómez

Sing to the Lord with joyful song





**Llamada
entrante**



**Llamamos de
soporte técnico,
necesitamos
acceso a tu
equipo**

Tipo	Descripción	Ejemplo
Email Phishing	Correos falsos que aparentan ser de bancos o jefes.	"Factura pendiente, abre el PDF"
Spear Phishing	Personalizado a una persona específica.	"Hola Juan, compra tarjetas de regalo para clientes"
Smishing	Phishing por SMS.	"Tu paquete está en espera, haz clic aquí"
Vishing	Llamadas fraudulentas.	"Llamamos de soporte técnico, necesitamos acceso a tu equipo"

. ¿Cómo Reconocer un Correo Falso?

Señales de alerta:




Link text

≡ Link text

http://c lint/balinke_clicing

http: Verifintc/clicktin: 20171
http:4000732inp

Redemail/adresss

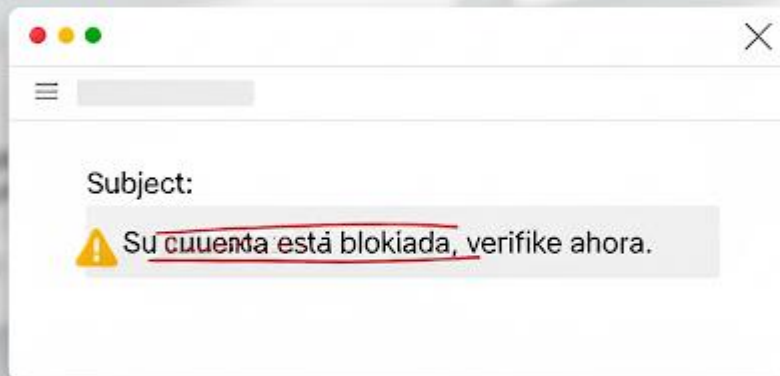
/@maildess

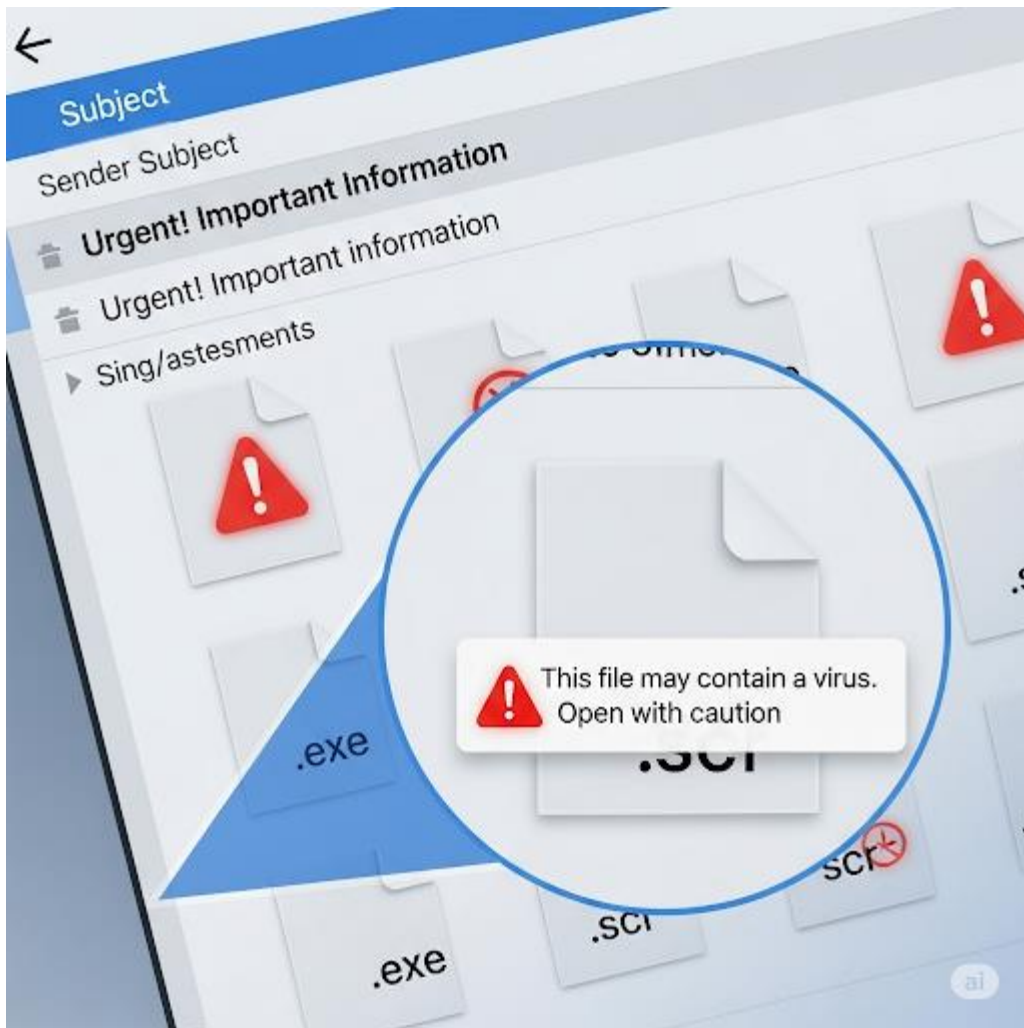
john123

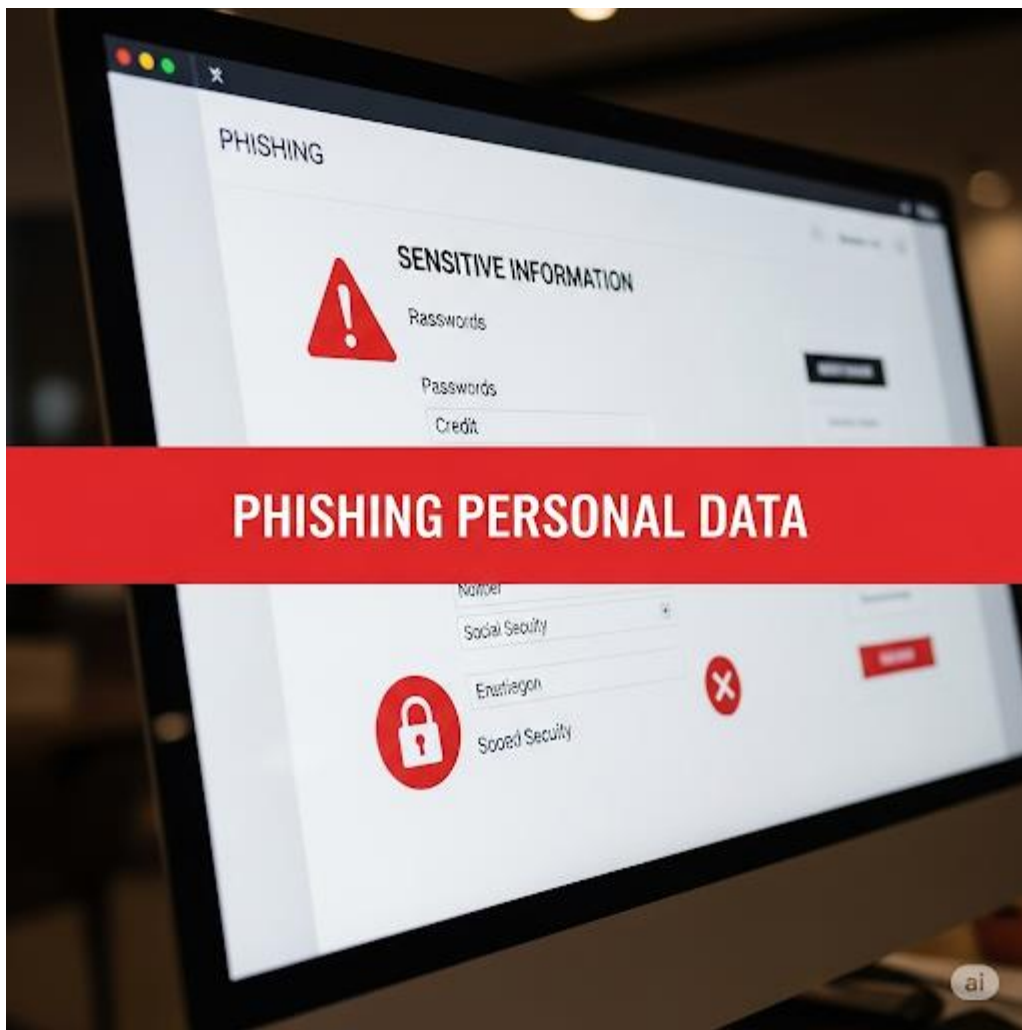


****bestdeals4u****

**bestdeals4u/odi/email/emill.com







- Dirección de remitente sospechosa
- Enlaces a páginas no oficiales
- Solicitud urgente de datos personales
- Archivos adjuntos sospechosos
- Errores gramaticales

TIP: Pasa el mouse por el enlace sin hacer clic para ver su destino real.

5. ¿Qué Hacer Si Recibes un Mensaje Sospechoso?

1. No hagas clic en enlaces
2. No respondas
3. No descargues archivos
4. Reporta al departamento de TI
5. Elimina el correo

6. Buenas Prácticas Empresariales

- Activar doble autenticación (2FA)
- Cambiar contraseñas regularmente
- Evitar redes Wi-Fi públicas
- Capacitar continuamente al personal
- Establecer políticas internas de seguridad

BUENAS PRÁCTICAS EMPRESARIALES



**Activar doble
autenticación (2FA)**



**Cambiar contraseñas
regularmente**



**Evitar redes
Wi-Fi públicas**



**Capacitar
continuamente
al personal**



**Establecer políticas
internas de seguridad**

QUÉ HACER SI RECIBES UN MENSAJE SOSPECHOSO



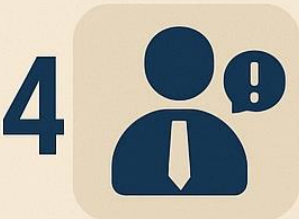
**No hagas clic
en enlaces**



No respondas



**No descargues
archivos**



**Reporta al
departamento de
TI**



Elimina el correo

