CIBERCONSEJOS PHISHING

¡CUIDADO CON LOS CORREOS FALSOS! CÓMO IDENTIFICAR Y EVITAR EL PHISHING

¡Tu seguridad digital, nuestra prioridad!

BICENTENARIO DE BOLIVIA

AGETIC
Digitalizando Bolivia

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE LA PRESIDENCIA

¿QUÉ ES EL PHISHING?

El phishing es una técnica de fraude cibernético empleada por ciberdelincuentes para obtener información confidencial haciéndose pasar por entidades legítimas. Utilizan correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos para engañar a las víctimas.

¿QUÉ DATOS BUSCAN OBTENER?

Datos personales

- Nombres y apellidos
- Cédula de identidad
- Fecha de nacimiento
- Dirección de domicilio
- Estado civil
- Número de celular
- Dirección de correo electrónico

Datos financieros

- Números de cuentas bancarias
- Números de tarjetas de crédito o débito
- Números de ingresos, salarios, patrimonio

El phishing puede ser muy sofisticado y difícil de detectar. Por eso, es esencial conocer sus formas y técnicas para proteger nuestra información.

TIPOS DE PHISHING

Phishing tradicional

Correos falsos que imitan a bancos o servicios.

Pharming

Páginas web falsas con URL engañosa.

Vishing

Llamadas telefónicas con engaños.

Smishing

Mensajes de texto con enlaces falsos.

Phishing por apps

Aplicaciones móviles falsas.

Spear phishing

Ataques personalizados con tus datos.

Whaling

Ataques a ejecutivos o directivos.

Clone phishing

Correos legítimos clonados con enlaces maliciosos.

QRishing

Códigos QR falsos que redirigen a páginas fraudulentas.

TÉCNICAS COMUNES DE PHISHING

Correos falsos de bancos

Solicitan actualización de datos con mensajes alarmistas y enlaces a sitios fraudulentos.

Premios falsos

Mensajes o llamadas que prometen premios inexistentes.

Notificaciones falsas de redes sociales

Solicitan reingresar contraseñas para verificar cuentas, simulan ser plataformas digitales conocidas.

Ofertas de trabajo falsas

Prometen salarios altos por trabajos sin esfuerzo.

Soporte técnico falso

Piden acceso remoto a tu computadora o descarga de aplicaciones supuestamente para solucionar problemas de virus.

Smishing

Mensajes SMS fraudulentos con enlaces o números falsos.

¿QUÉ HACER SI FUISTE VÍCTIMA DE PHISHING?

Cambia tus contraseñas

Hazlo inmediatamente en todas tus cuentas, y usa contraseñas seguras con autenticación de dos factores (2FA).

Contacta a las instituciones que suplantó el ataque

- **Departamento de TI** (si es una organización).
- **Tu banco o entidad financiera.**
- **Plataformas digitales** (redes sociales, correo electrónico, apps).

Informa y denuncia a las autoridades

- **Bloquea la Estafa – ATT:**

https://bloquealaestafa.att.gob.bo.

- **División de Cibercrimen – Policía Boliviana.**

Revisa la actividad de tus cuentas

Revisa transacciones bancarias, correos y redes sociales frecuentemente.

Documenta

Guarda copias, capturas de pantalla y detalles del ataque (correos, sitios, mensajes, etc.).

Escanea tus dispositivos

Utiliza antivirus confiable para detectar y eliminar el malware (Software malicioso).

CONCLUSIÓN

Nunca proporciones datos personales, bancarios u otras, estas pueden ser utilizadas para afectar tu patrimonio.

Educa a otros

Comparte tu experiencia para ayudar a prevenir más víctimas.

AGETIC
Digitalizando Bolivia

¿DUDAS DE UN MENSAJE? NO LO ABRAS, NO LO RESPONDAS, NO LO COMPARTAS. TU SEGURIDAD DIGITAL DEPENDE DE TI

Agetic Bolivia
(+591) 63124081
(+591) 63124081