ISO/IEC 27001:2013

SEGURIDAD DE LA INFORMACIÓN

Tribunal Electoral de la Provincia de Misiones

Febrero 2022 N° - 001/22

Phishing

El phishing es una técnica que consiste en engañar al usuario para robarle información confidencial, claves de acceso, etc., haciéndole creer que está en un sitio oficial o de total confianza.

¿Que Información Buscan?

- **Datos Personales:**
  - Dirección de correo electrónico
  - Numero de documento de identidad
  - Datos de localización y contactos
- **Credenciales de Acceso**
  - Redes sociales
  - Cuentas de correo electrónico
- **Información Financiera**
  - Numero de tarjetas de créditos/débito
  - Numero de Cuentas
  - Información de home banking

Principales medios de Propagación

- Correo electrónico
- Redes sociales

- SMS - Llamadas telefónicas
- Infección de malware - Virus

Ejemplos de Phishing

```
----- Mensaje reenviado -----
De: "sistema de administrador" <adriana.scattareggiamarchese-esterno@izslt.it>
Para: "Recipients" <adriana.scattareggiamarchese-esterno@izslt.it>
Enviados: Lunes, 7 de Febrero 2022 17:00:06
Asunto: Estimados usuarios de correo electrónico,

Estimados usuarios de correo electrónico,

Tu buzón ha superado los 20.362 en su cuota. No puedes
enviar o recibir nuevos mensajes hasta que vuelva a validar su cuota de buzón. Para
renovar la cuota de su buzón. Por favor Haga clic aquí para aumentar la cuota de su
buzón.

https://www.tekbuff.com/wm/

¡Advertencia temprana!
De lo contrario, solo el buzón tendrá acceso limitado.
Si no actualiza la cuota de su cuenta dentro de las 24 horas
su cuenta de correo electrónico será deshabilitada.
```

electoralmisiones.gov.ar

Hola oantonio,

Recientemente hiciste una solicitud para desactivar **oantonio@electoralmisiones.gov.ar** como en **2/4/2022 5:30:38 a.m.** .Esta solicitud sera procesada en breve.
Si no hizo esta solicitud, cancele amablemente la solicitud ahora.

Cancelar la desactivacion

Si no cancela esta solicitud, su oantonio@electoralmisiones.gov.ar Se desactivara y se perderan todos sus datos de correo electronico.

Www.electoralmisiones.gov.ar (c) 2022.

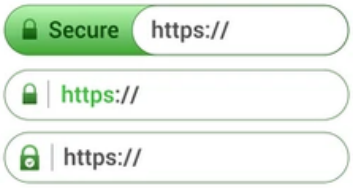
Detección y Prevención

- VERIFICA LA FUENTE DEL CORREO ELECTRÓNICO.

Tu banco no te pedirá que le envíes tus **claves** o **datos personales** por correo. Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente a tu banco para asesorarte.

- INTRODUCE TUS DATOS CONFIDENCIALES ÚNICAMENTE EN WEBS SEGURAS

Las webs seguras han de empezar por **'https://'** y debe aparecer en tu navegador el icono de un pequeño candado cerrado.



- EL PHISHING NO SABE IDIOMAS

Por lo general se encuentran **mal escritos** o **traducidos**, así que lo podemos considerar como un indicador de un posible fraude.

Si **nunca** entras a la web en **inglés** de tu banco, ¿Por qué ahora debe llegarte un comunicado suyo en este idioma?

- ANTE LA MÍNIMA DUDA SE PRUDENTE Y CONSULTA CON LA SECRETARIA DE TIC.

La mejor forma mas segura siempre es **rechazar** de forma sistemática cualquier correo electrónico o comunicado que **solicite datos confidenciales**.

Elimina este tipo de correos y comunicarle al área de **soporte técnico** para que pueda brindarte **ayuda**.