IEEG
INSTITUTO ELECTORAL
DEL ESTADO DE GUANAJUATO

UTSIT

Tipo de ciberataque

PHISHING

¿Qué es phishing?
Atacantes que se hacen pasar por una entidad genuina.

¿Qué hace?
Instala malware (programa malicioso) para obtener información confidencial.

Tipos de ataque de phishing
Emails, clonación, llamadas telefónicas, etc.

¿Cómo identificar un ataque de phishing?
Mensajes con archivos adjuntos, enlaces a páginas con URLs sospechosas.
Llamadas de dudosa procedencia haciéndose pasar por instituciones bancarias, de mensajería o paquetería u otras que pidan información personal o confidencial.

¿Cómo protegerse del phishing?

- No abra correos electrónicos de remitentes que no le sean familiares.
- No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.
- Busque el certificado digital del sitio web.

Da click aquí para conocer más

- Pase el cursor del ratón por encima del enlace para ver si es legítimo.

Ver ejemplo

- Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no se tiene seguridad, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en su navegador.
- No atienda llamadas telefónicas de números desconocidos, o bien, si las atiende no brinde información que debiera estar en poder de quien llama al ser una empresa con la cual usted tiene algún tipo de servicio contratado.

