PHISHING

Es una forma de ingeniería social, en la cual el atacante envía correos electrónicos que suplantan a entidades, empresas conocidas o terceros de confianza, para lograr engañar a los usuarios bajo cualquier excusa y poder robar sus datos personales, bancarios, contraseñas o cualquier información confidencial.

¿Cómo puedo evitar caer?

- **No abrir ni contestar** correos que procedan de usuarios desconocidos.
- **Mantener actualizados** todos los dispositivos y programas.
- **No hacer clic en enlaces** incluidos en correos electrónicos sin antes verificar dentro de VirusTotal a qué sitio web te redirige ese enlace.
- **No descargar** archivos adjuntos de correos sospechosos o desconocidos.
- **Utilizar** software de seguridad como un **antivirus y mantenerlo actualizado** para proteger los dispositivos.

Algo que debes saber:

- Tu banco **no te va a solicitar tus datos personales** a través del correo electrónico u otros medios. **Verifica** la fuente de información de tus **correos entrantes**.
- Antes de introducir información confidencial en una página web, **asegúrate que es segura**. La dirección Web debe de iniciar con **https://** y tener un candado cerrado en el navegador.
- **Aprende** a identificar correctamente correos electrónicos Phishing: Generalmente **solicitan** información con urgencia y confidencial, así como también, errores de ortografía y/o mensajes incoherentes, confusos o saludos genéricos.
- **Activa** la autenticación de **dos pasos** en tu correo electrónico y también en las plataformas o servicios que lo permitan.

¿Cómo identificar un correo electrónico Phishing?

1. **Remitente**
   ¿Esperabas un email de esta persona?
   Comprueba que el email coincida con quien dice ser o si está suplantando a alguien.
2. **Asunto**
   ¿Capta tu atención?
   La mayoría de correos fraudulentos utilizan asuntos llamativos para captar tu atención.
3. **Objetivo del correo**
   ¿Qué está buscando obtener de ti?
   Un banco u otro servicio no pedirá tus datos personales por correo. Si se está usando la urgencia, amenazas u ofertas muy atractivas, puede ser fraude.
4. **Redacción**
   ¿Tiene errores ortográficos o parece una traducción de otro idioma?
   Revisa la redacción, busca errores gramáticos u ortográficos. Y mira si no está personalizado o parece una traducción automática.
5. **Enlaces**
   ¿Los enlaces llevan a una página legítima?
   Antes de acceder a cualquier enlace, cópialo haciendo clic derecho sobre él y pégalo en la barra buscadora o en el apartado de URL dentro de VirusTotal, si el enlace no sale limpio no hagas clic.
6. **Adjuntos**
   ¿Contiene un archivo que no estabas esperando o es sospechoso?
   Analiza los adjuntos antes de abrirlos, los antivirus y analizadores de ficheros te pueden ayudar.

URL a la página de VirusTotal:

Smishing

Es un término que se utiliza para describir una forma de fraude en la que los delincuentes intentan engañar a las personas para que compartan información personal o financiera enviándoles mensajes de texto (SMS) que incorporan enlaces fraudulentos.

Vishing

Es un término que se refiere a engañar a los usuarios a través de llamadas de teléfono fraudulentas y obtener así información personal sobre ellos, guiarles para que descarguen e instalen programas maliciosos, así como intentar que realicen algún pago bajo algún pretexto.

¿Cómo debo actuar?

Lo primero que debes hacer es ¡no responder a la petición del email sospechoso! y lo siguiente sería acercarse a la empresa que supuestamente te está contactando, a través de sus canales oficiales para confirmar su comunicado.

¿Has caído en el engaño? Sigue estas recomendaciones:

- **Asegúrate de que tus contraseñas sean robustas** y no reutilices contraseñas pasadas.
- **Cambia tus contraseñas** si proporcionaste información de inicio de sesión.
- **Contacta con tu banco** o entidad financiera si facilitaste datos bancarios.
- **Escanea tu dispositivo** si pulsaste en algún enlace o descargaste algún archivo.
- **Realiza búsquedas en Internet** de tus datos personales para comprobar que no se estén usando.
- **Ejerce tus derechos** si encuentras algún dato tuyo que se está ofreciendo sin tu consentimiento.
- **Comparte tu experiencia con amigos y familiares** para ayudarles a evitar caer.
- **Reenvía el correo** fraudulento a **seguridadinf@itson.edu.mx** para poder concientizar.