PHISHX

CONSEJOS PARA EVITAR EL *PHISHING* Y EL *MALWARE*

Ten cuidado con los mensajes sospechosos

El nombre y la dirección del remitente que aparecen en el mensaje se pueden modificar fácilmente para mostrar información falsa. Las compañías y bancos legítimos no envían mensajes sin el registro y consentimiento adecuados, en ninguna circunstancia. Por lo tanto, no crea en mensajes de fuentes que no haya registrado y aprobado previamente. En caso de duda, obtenga una segunda opinión. Acceda directamente al sitio web de la empresa o a los canales de contacto oficiales.

Ten cuidado con las grandes ofertas

Tan tentador como ese viaje súper barato, esa promoción imperdible o ese correo electrónico lleno de preguntas que promete eliminar todas las dudas con un simple "clic aquí", ¡sospeche! Ahí es donde se esconden las trampas, que lo ponen a usted y a su compañero de trabajo en riesgo. Recuerde los canales oficiales de la compañía para divulgar beneficios a los usuarios.

Tenga cuidado con la urgencia y los plazos

Provocar un sentido de urgencia o miedo es una táctica común. Tenga cuidado con los mensajes que atraen demasiado su atención y que, de alguna manera, lo amenazan si no sigue los procedimientos descritos. Esté atento a los mensajes, recibidos en nombre de una institución, que intentan engañarlo para que brinde información, instale / ejecute programas o haga clic en los enlaces.

PHISHX

CONSEJOS PARA EVITAR EL *PHISHING* Y EL *MALWARE*

Cuidado con enlaces y archivos adjuntos

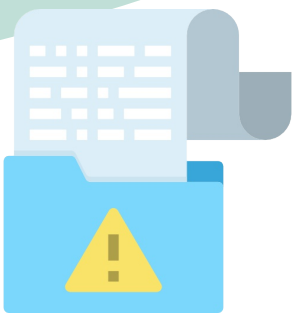
Cuando reciba un mensaje cuestionable, no acceda a los enlaces ni ejecute los archivos adjuntos.
Verifique el enlace que se muestra en el mensaje. Los estafadores a menudo usan técnicas para ocultar el vínculo real con el phishing. Al colocar el ratón sobre el enlace, a menudo es posible ver la dirección real de la página falsa o código malicioso.
Si la dirección del enlace parece extraña, ¡no hagas clic en ella!

No ejecutes archivos innecesarios

Si recibiera una caja de bombones por correo de una persona desconocida, ¿la abriría y se la comería sin dudarlo? Probablemente no. Asimismo, es importante tener cuidado cuando una persona desconocida envía un correo electrónico sospechoso que contiene archivos adjuntos e imágenes.
Algunos sitios web y aplicaciones le permiten compartir fácilmente archivos con otros usuarios. Muchos de estos sitios y aplicaciones ofrecen poca protección contra el malware. Si comparte o descarga archivos utilizando estos métodos para compartir, tenga en cuenta el malware. El malware puede disfrazarse de película, álbum, juego o programa popular.

Lea el contrato detenidamente

Parece algo aburrido, y realmente lo es. Sin embargo, es necesario. Algunos contratos o términos, que aceptamos sin leer, autorizan que nuestra información guardada en la máquina se envíe a terceros para que tengan acceso.
Y luego sabemos lo que puede suceder: la invasión.



phishx.io