SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
ONE TELECOMUNICACIONES SAS

Teniendo en cuenta la importancia que como cliente de nuestro servicio de internet mediante este documento le informamos las modalidades de vulneración al servicio de internet, su red y a su información más comunes que se pueden llegar a presentar y la forma en la que pueden ser mitigados:

PHISHING

Definición:

El "phishing" es una modalidad de estafa diseñada con la finalidad de apropiarse o robar la identidad del usuario. Este acto delictivo consiste en obtener información del usuario a través de engaños y relacionados con tarjetas de crédito, contraseñas, información de cuentas u otros datos personales. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

Cómo funciona el "phishing":

En este tipo de fraude, el usuario malintencionado o delincuente envía millones de mensajes con información falsa y con el fin de dar la apariencia que los mismos provienen de sitios Web reconocidos o de su confianza tales como su banco o la empresa de su tarjeta de crédito. Dado el nivel de detalle y/o a la información contenida en los mensajes y los sitios Web que son envíados estos usuarios aparentan ser los oficiales y logran engañar a muchas personas haciéndoles creer que son legítimos por lo que el cliente o usuario del sitio web confía normalmente y responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Los delincuentes para aparentar ser legítimos suelen incluir un vínculo (link) falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente clonada o copia del sitio Web oficial ("sitios Web piratas"). Una vez que el usuario está en uno de estos sitios Web, ingrese su datos de perfil y contraseña y sin conocer la realidad del sitio al que accedió transmite sus datos personales al delincuente quien las utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Cómo Protegerse del "phishing

Este tipo de fraude debe contener a través de las actuaciones que adelante ONE TELECOMUNICACIONES SAS y también es responsabilidad del usuario de nuestros servicios de conectividad a internet.

Es responsabilidad del usuario de servicios de conectividad a internet que oferta ONE TELECOMUNICACIONES SAS para evitar que sea víctima de robo de su identidad y en consecuencia llevar a cabo las siguientes actuaciones:

- Nunca responda a solicitudes de información personal a través de correo electrónico y proceda a comunicarse con la entidad que supuestamente le ha enviado el mensaje.
- Debe tener especial cuidado con correos supuestamente enviados por entidades financieras y plataformas de compra online (amazon, temu, shopee, alibaba, ebay, paypal ect)
- Debe tener especial cuidado con correos que soliciten actualizar datos de cuentas y/o accesos sin que usted haya realizado la solicitud formal.
- Asegúrese que el dispositivo(Tablet, pc, celular) desde el que usted se conecta a nuestro servicio de internet tenga las últimas actualizaciones a nivel de seguridad del fabricante y cuente con el respectivo antivirus.
- Se recomienda a la hora de navegar digitar en la barra de direcciones la dirección URL del sitio web al que desea acceder
- Verificar que el sitio Web que usted visita utiliza cifrado
- En caso dado que tenga instalado servidores Web debe asegurarse que tanto el aplicativo como el sistema operativo del mismo cuenten con las últimas actualizaciones a nivel de seguridad establecidas por el fabricante.
- Informar a ONE TELECOMUNICACIONES SAS y a la fiscalía general de la Nación el o los posibles delitos relacionados con su información personal a las autoridades competentes.

SPAM

Definición:

Se llama spam o correo basura a todos aquellos mensajes no solicitados que habitualmente son de tipo publicitario y que son enviados en cantidades masivas por parte de personas no identificadas ni conicidad y que copan la capacidad de almacenaje del correo electrónico del usuario.

ONE TELECOMUNICACIONES SAS hace lo posible para bloquear las URL'S que son reportadas por el envío de SPAM, sin embargo el usuario de nuestros servicio de internet puede llevar a cabo las siguientes actuaciones:

- Tenga en cuenta que si no se reconoce el remitente de un correo, no abra el mismo ya que los archivos adjuntos al mensaje pueden tener archivos maliciosos.
- Usted puede instalar un software bloqueador de spam.
- Si usted no conoce el remitente y observa que la información contenida en el mensaje no tiene relación con usted o es publicidad no solicitada o puede ser perjudicial para usted designela como SPAM o correo no deseado.
- Nunca dé clic sobre enlaces (links) que se encuentren dentro de un mensaje de correo electrónico proveniente de un remitente desconocido.
- Si desea acceder a un enlace (link) dentro del mensaje, recomendamos en aras de evitar fraude, que digite la URL del sitio web a visitar y consulte la información.
- Con el fin de evitar que su cuenta sea ingresada en listas de correo utilizadas por los spammers, es necesario que usted esté atento a los

dominio o sitios en los que ingresa y que le piden registrarse a través de la inclusión de su cuenta de correo

- En caso que usted desee verificar si un correo electrónico está registrado en las listas negras de spam puede visitar el siguente sitio web: http://www.dnsstuff.com/
- En caso dado que su IP haya sido reportada en las las listas negras de spam puede acceder al siguiente enlace para tramitar el desbloqueo: http://200.118.2.73/varios/bloqueoIPs.asp.
  Tenga en cuenta que el bloqueo solo será efectivo si el titular del correo electrónico toma las medidas necesarias para evitar que se continúe enviando correo spam.

A continuación relacionamos el tiempo de desbloqueo en el que puede darse el desbloqueo de una IP que ha sido reportada:

www.aol.com: Tiempo de desbloqueo aprox. 48 horas

www.lashback.com: Tiempo de desbloqueo aprox. 1 hora

www.uceprotect.net: Tiempo de desbloqueo aprox. 7 días

www.spamcop.net: Tiempo de desbloqueo aprox. 24 horas

www.dsbl.org: Tiempo de desbloqueo aprox. 7 días

WWW.WPBL.INFO: Tiempo de desbloqueo aprox. 1 hora

WWW.MOENSTED.DK: Tiempo de desbloqueo aprox. 1 hora

www.comcast.com: Tiempo de desbloqueo aprox. 48 horas

www.abuso.cantv.net: Tiempo de desbloqueo aprox.48 horas

www.spamhaus.org: Tiempo de desbloqueo aprox. 24 horas

VIRUS

Definición:

Un virus informático es un programa que se copia de forma automática y busca modificar sin permiso del propietario del dispositivo de conexión al servicio de internet (pc, celular, tablet) con el fin de afectar el normal funcionamiento de este equipo. Es importante que tenga en cuenta que los virus pueden llegar a destruir, de manera intencionada, los datos que se encuentran almacenados en el dispositivo de conexión al servicio de internet (pc, celular, tablet) pueden propagarse, replicándose con distintos objetivos.

Cómo protegerse de un Virus:

ONE TELECOMUNICACIONES SAS hace lo posible para bloquear los virus más conocidos, sin embargo usted como usuario de nuestros servicio de internet puede llevar a cabo las siguientes actuaciones:

- En caso dado que usted no reconozca un remitente de un correo, no abra ninguno de los archivos adjuntos al mismo, sin importar que usted tenga un antivirus ejecutándose en su dispositivo de conexión.

- Evitar que en su dispositivo de conexión se lleve a cabo la instalación de software pirata o de baja calidad.
- Tenga en cuenta que su dispositivo de conexión debe contar con las últimas actualizaciones a nivel de seguridad tanto a nivel de sistema operativo como de las aplicaciones instaladas.
- Instalar un software antivirus dispositivo de conexión y que el mismo esté actualizado