RECOMENDACIONES DE SEGURIDAD PARA USUARIOS DE STARNET TECHNOLOGY SAS

El sistema de gestión de seguridad de la información basado en la ISO 27001 para StarNet se implementa con el fin de dar mayor seguridad a la información de todos los usuarios de StarNet.

El siguiente documento trata los temas de protección de seguridad y confidencialidad de la información en los siguientes temas:

Es importante aclarar que el primer filtro ante un ciberataque es el usuario final, el éxito del ataque dependerá de conocimiento o desconocimiento de los usuarios de StarNet, por esta razón se detalla a continuación los diferentes ataques y contramedidas para una mayor seguridad de la información.

StarNet
TECHNOLOGY S.A.S

Correos

Los correos electrónicos son un punto de ataque, no se recomienda usarse para registrarse a cualquier página de internet, estos pueden ser usados para el envío masivo de correos publicitarios o el envio de virus adjunto en archivos.

Caso real: el usuario puede llegar a recibir un correo sospechoso, dentro de este correo vendrá un archivo adjunto, este archivo contiene una versión nueva de ransomware, el usuario descargará y ejecutará el archivo, esto causará que toda la información sea cifrada y que todos los equipos en la red sean infectados de igual manera.

¿cómo prevenir este tipo de ataques?

- Evitar abrir correos electrónicos de dudosa procedencia.
- No descargar ni ejecutar ningún archivo adjunto de correos electrónicos que no se han solicitado.
- Si el archivo y el correo electrónico son de confianza pero tiene dudas sobre los archivos adjuntos comuníquese con el area de tecnologia.

Navegación segura

No todas las páginas web son seguras, para saber si una página web lo es, es importante saber que estas deben contener en su URL el protocolo https NO http, cabe aclarar que una página web que usa el protocolo https garantiza que todo el tráfico que pasa por ella va cifrado y con esto hablamos de lo más importante que son las credenciales de un usuario.

Caso real: un usuario ingresa a la página del banco Bancolombia desde un link que encontró en una página web diferente y ajena a la del banco, la pagina web es www.mibanco.bancolombia.123.com.es ingresa sus credenciales y estas son robadas por un pirata informático, este ataque es llamado phishing.

¿cómo prevenir este tipo de ataques?

- No ingrese a páginas web de bancos o páginas que usen usuario y contraseña sin que esta use el protocolo https.
- Verifique que la página web contenga un candado o un certificado válido.
- Verifique que la URL a la que está ingresando es la oficial.
- No abra POP UPs o ventanas emergentes en páginas web sospechosas.
- Si la página web a la que está ingresando no cumple con los parámetros de seguridad no ingrese sus datos personales o credenciales de acceso.
- Use doble factor de autenticación, las contraseñas ya no son seguras.
- Use contraseñas seguras, robustas.

Contraseñas seguras

El uso de contraseñas robustas evita en un alto porcentaje que nuestras cuentas sean robadas o pirateadas, una contraseña segura contiene letras, número, caracteres especiales y mayúsculas.

Nunca se debe usar información personal para crear una contraseña, información tal como nuestro nombre, nuestra cédula de ciudadanía, teléfono

fijo o celular, nombre de mascota o hijos, deportes favoritos, gustos entre otros.

¿Cómo crear una contraseña robusta?

Es tan sencillo como esto, crear una contraseña segura para algunas personas puede llegar a ser un dolor de cabeza, pero siguiendo estos pasos será mucho más fácil.

- Inicia con un carácter especial, * $ # entre otros.
- Usan una mayúscula al inicio y al final.
- Puedes usar nombres pero cambia las vocales por números por ejemplo la “i” por un “1” la “o” por un “0” cero.
- cambia tu contraseña periódicamente.

Tipos de virus

Existe un sin fin de virus informáticos en el mundo, pero se puede llegar a clasificar en los siguientes:

Adware: Un adware es un software que muestra anuncios. “Los adware se instalan generalmente sin que nosotros lo deseemos.“Los adware suelen rastrear nuestro uso del ordenador para mostrar publicidad que tiene que ver con nuestras búsquedas en diferentes buscadores o relacionados con los sitios que visitamos”.

Spyware: El spyware es un software espía que recopila información de un ordenador. “Tras obtener los datos, los transmite a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador”

Ransomware: Consiste en que el pirata bloquea el smartphone u ordenador con un mensaje en el que solicita un rescate para liberarlo. El usuario debe pagar dicho rescate en la moneda digital Bitcoin, para que no se pueda rastrear y se mantenga el anonimato del pirata.

Gusanos: Tiene la capacidad de replicarse en un sistema, por lo que el ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.

Troyano: Se trata de un tipo de programa que contiene otro dentro de él, al ejecutarlo instalará el virus en el ordenador, se suele ver comúnmente en activadores, cracks o KeyGens.

StarNet
TECHNOLOGY S.A.S

Unidades de red

Las unidades de red permiten a un grupo de usuarios compartir información de manera rápida, pero en algunas ocasiones estas carpetas pueden llegar a ser el punto de infección ante un potente virus o el lugar donde se encuentre la mayor cantidad de pirateria y conllevar a una sanción por parte de la DIAN por uso de software ilegal o la violacion de derechos de autor por contener música, videos, libros o cualquier contenido con CopyRight.

Las sanciones pueden ser una pena de 2 a 5 años de prisión o de 20 a 1000 salarios mínimos vigentes, el delito es denominado Defraudación a los Derechos Patrimoniales del Autor y es controlado por La DIAN (Dirección de Impuesto y Aduanas Nacionales)

¿Cómo evitar esto?

- Evitar contener software ilegal.
- Periódicamente buscar y limpiar todo tipo de archivo que infrinja esta política.
- Para evitar propagación de virus, usar protocolos seguros.

Antivirus

Los antivirus son programas avanzados diseñados para defender nuestros dispositivos de los comúnmente llamados virus informáticos. Estos contienen distintos módulos que nos ayudan a mantener seguro nuestros equipos, entre estos módulos podemos encontrar:

- Anti-phishing
- Control parental
- Anti-malware
- Anti-Ransomware
- VPN

Entre otros módulos avanzados, se recomienda tener un antivirus actualizado y de pago no gratis, crackeado o activado con keyGens.

Medios de almacenamiento externo

Se conoce como medio de almacenamiento externo todo dispositivo como (USB, disco portable, MicroSD, entre otros sistema de almacenamiento externos), es recomendable analizar y desinfectar cualquier dispositivo que se conecte a nuestro ordenador, estos pueden ser quienes infecten nuestro sistema operativo, cabe aclarar que todos los sistemas operativos son vulnerables a virus, como Windows, Linux y MacOS. Utiliza un buen antivirus.

Actualizaciones del sistema operativo

Es muy importante mantener nuestro sistema operativo actualizado, por lo general todos los fabricantes liberan constante y periódicamente actualizaciones parchando vulnerabilidades y fallos en los sistemas.

Esto lo hacemos con el fin de lograr mayor seguridad y evitar que un nuevo virus afecte nuestros dispositivos.

Conexión Wi-FI

Todos usamos conexiones Wi-Fi ya sea en nuestros lugares de trabajo en en nuestros hogares, pero la navegación debe ser segura en todo momento, no podemos usar una red vulnerable o vulnerada y hacer nuestras transacciones bancarios sin prestar atención a ello, una red Wi-Fi insegura es aquella que está abierta o sin contraseña, una red que no cambia periódicamente su clave, que usa cifrados débiles como el WEB, este tipo de cifrado es fácil de vulnerar, solo basta con hacer un ataque de fuerza bruta y eso seria todo.

Nuestra Wi-Fi debe estar segura, alguien podría entrar en nuestra red y cometer un delito sin que nosotros lo sepamos y ser nosotros quienes tengamos que responder ante las autoridades por ser quienes contratamos el servicio.

Es recomendable, no compartir la clave Wi-Fi con todos, es recomendable cambiar la clave periódicamente, saber cuantas personas están conectadas a nuestra red.