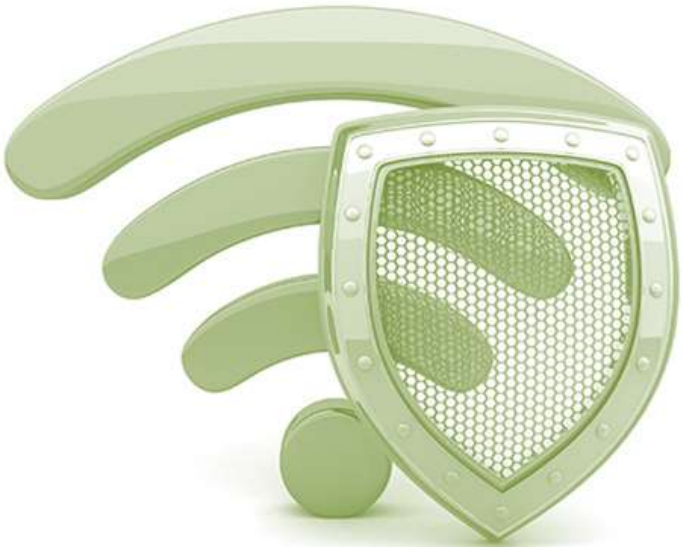
SEGURIDAD EN LA RED



Internet es la red de redes, por la cual, millones de computadoras se pueden conectar entre sí y provee una amplia variedad de posibilidades de comunicación, interacción y entretenimiento. Por este motivo se deben implementar mecanismos que protejan y reduzcan los riesgos de seguridad a través del mismo servicio de internet. Para ello se implementa la seguridad de redes que es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos. Por ello es necesario estar alertas para prevenir fraudes que puedan realizar a través de la red.

MECANISMOS DE SEGURIDAD

TV ISLA LTDA cuenta con diferentes protecciones para las plataformas de servicios de internet tales como firewalls, mecanismos de autenticación por dirección IP y MAC por usuario.

Todas las estaciones de trabajo, así como los servidores de procesamiento, monitoreo, control y almacenamiento en TV ISLA LTDA son protegidos a través de antivirus.

TV ISLA LTDA ha implementado configuraciones de seguridad en todos los equipos de red como una línea base de seguridad y realiza monitoreo del tráfico que pueda resultar nocivo.

Los clientes pueden realizar filtrado de URL's a través de sus navegadores web, se sugiere instalar además sistemas de control parental.

TV ISLA LTDA cuenta con herramientas de control para todo el tráfico de internet con el fin de bloquear toda página que contenga o promueva la pornografía infantil en internet de cualquier manera.

Los dispositivos de conexión final ubicados en el lugar del cliente cuentan con características de bloqueo básico que pueden ser solicitados llamando a nuestra línea de atención gratuita por el titular del servicio. Adicionalmente cuentan con un sistema de autenticación y autorización para realizar una conexión a internet más segura.

TIPOS DE FRAUDES

Malware

Es un término general que se utiliza para referirse a distintas formas de software hostil, intrusívo o molesto.

El software malintencionado o malware es un software creado por hackers para perturbar las operaciones de una computadora, obtener información confidencial o acceder a sistemas informáticos privados.

El malware incluye virus informáticos, gusanos, troyanos, spyware, adware, la mayoría de rootkíts y otros programas malintencionados.

Las siguientes son algunas formas de software malintencionado:

Spyware

Es un tipo de malware (software malintencionado) que se instala en las computadoras para obtener información sobre los usuarios sin que éstos lo sepan. El spyware suele estar oculto al usuario y puede ser difícil de detectar.

Algunos spywares, como los keyloggers —registradores de teclas—, pueden ser instalados de forma intencionada por el propietario de una computadora de uso común, corporativo o público para controlar a los usuarios.

Aunque el término "spyware" sugiere un software que espía las actividades de un usuario en una computadora, las funciones del spyware pueden ir mucho más allá y llegar hasta la obtención de casi cualquier tipo de datos, incluida información personal como hábitos de navegación en Internet, accesos de usuarios o datos de crédito y cuentas bancarias. El spyware también puede interferir con el control de una computadora por parte del usuario, instalando nuevo software o redirigiendo a los navegadores web. Algunos spywares tienen capacidad para modificar la configuración de una computadora, lo que puede tener como consecuencia una menor velocidad de conexión a Internet y cambios no autorizados en la configuración de navegadores u otro software.

PHISHING

El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle al usuario su identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como un banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales,

logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aún más reales, el estafador suele 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 que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

PHARMING

Es una forma de ataque cuyo objetivo es redireccionar el tráfico de un sitio web hacia una página fraudulenta.
El término "pharming" es un neologismo formado por la unión de las palabras inglesas "phishing" y "farming". El phishing es una técnica de ingeniería social que pretende obtener datos de acceso, como nombres de usuarios y contraseñas. Tanto el pharming como el phishing se han utilizado en los últimos años con el fin de adquirir información que permita el robo de identidades online. El pharmíng es ya un problema grave para las empresas de comercio electrónico y banca electrónica.

Como Protegerse:

Este tipo de fraude debe contenerse a través del ISP y vía usuario.

El usuario debe seguir estas recomendaciones para evitar que sea víctima de robo de su identidad:

Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje. Tener especial cuidado en correos que supuestamente han sido enviados por entidades financieras y compras por Internet, como eBay, PayPal, bancos, etc. Solicitando actualizar datos de cuentas y/o accesos, ya que ninguna de estas entidades solicitan este tipo de información por este medio.

Asegúrese que su PC cuente con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes (Microsoft, Mac, etc…) Para visitar sitios Web, introduzca directamente la dirección URL en la barra de direcciones.

Asegúrese de que el sitio Web utiliza cifrado.

Si tiene instalado servidores Web, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. Muchas veces los phishers buscan en la red servidores Web vulnerables que puedan ser utilizados para montar páginas que intentan suplantar la identidad de una entidad financiera, sin que el usuario se de cuenta. Para el cliente, esto tiene como repercusión la afectación directa en su servicio de Internet, ya que la IP donde se encuentra alojada la página fraude es reportada por entidades internacionales pidiendo al ISP el bloqueo de la misma.
Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

SPAM

Se llama spam, correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera a los usuarios que reciben este correo. Aunque su difusión se puede hacer por distintas vías, lo más común es hacerlo vía correo electrónico.

Norma básica para evitar y reducir al mínimo el spam:

El spam es un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarios como a nivel de los proveedores de Internet.

A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser inundado por correo spam:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software bloqueador de spam y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC, desde borrar su información más valiosa hasta capturar contraseñas, números de tarjetas de crédito, etc… sin que el usuario ni siquiera se entere. Estas aplicaciones no se pueden incluir en un mensaje de correo electrónico en texto plano, la cual es la razón por la que se empaquetan en los archivos adjuntos.

Si recibe un correo spam, nunca haga clic en el vínculo “Quitar spam”, ya que lo que buscan los spammers es que el cliente verifique que esta dirección de correo está activa, añadiendo posiblemente su cuenta de correo a más y más listas de spam, lo cual ocasionará que usted reciba mayor cantidad de correo no deseado.

Algunos programas que utilizan los spammers tratan de adivinar las cuentas de correo a las cuales enviar correo no deseado, por lo cual es recomendable utilizar cuentas que contengas números y letras para que no sean fácilmente ubicadas.

Nunca dar clic sobre enlaces (links) que se encuentren dentro de un mensaje de correo electrónico de un remitente desconocido. Probablemente pueda ser un caso de phishing para tratar de robar la identidad del usuario o puede activar un programa que silenciosamente descargue aplicaciones en su PC.

En caso de que usted conozca al remitente, igual la recomendación es no dar clic sobre enlaces (links) que se encuentren dentro del mensaje. Uno nunca puede estar seguro de que quien envía el mensaje es realmente quien dice ser, ya que los spammers pueden cambiar la cuenta remitente, suplantando la identidad de otra persona.

Para acceder a un enlace (link) dentro del mensaje, se recomienda cerrar el mensaje, y visitar el sitio en cuestión, introduciendo manualmente la URL (por ejemplo, www.google.com) en su navegador de Internet. Es la única manera de estar seguro que la página a la cual se está accediendo es la real.

Para tratar de evitar que su cuenta sea ingresada en listas de correo utilizadas por los spammers, se recomienda que el usuario preste cuidado a los sitios donde ingresa y que le solicita registrarse (mediante una cuenta de correo), ya

que existen muchos sitios Web inescrupulosos que venden estas cuentas registradas a redes de spammers.

Si tiene instalado servidores de correo, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. En muchos casos, los servidores de correo, debido a configuraciones deficientes, permiten que cualquier persona, desde Internet, utilice estos servidores para enviar correos (conocido como Open Relay), afectando el servicio de correo del cliente y muy posiblemente será bloqueado en listas negras de Spam mantenidas a nivel mundial.

VIRUS

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del PC, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un PC aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Como Protegerse:

Similar al spam, los virus son un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarios como a nivel de los proveedores de Internet.

A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser víctima de los efectos de un virus informático:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software antivirus y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC. Evite caer en técnicas conocidas como de Ingeniería social en la cual llega un correo electrónico con un mensaje del estilo "ejecute este programa y gane un premio".

Evitar la instalación de software pirata o de baja calidad, mediante la utilización de redes P2P, ya que muchas veces, existen ciertos sitios que "prometen" la descarga de un aplicativo en particular pero en realidad lo que el usuario descarga es un virus.

Asegurarse que su equipo PC cuente con las últimas actualizaciones a nivel de seguridad tanto a nivel de sistema operativo como de los aplicativos instalados, dadas por el fabricante. Existen algunos tipos de virus que se propagan sin la intervención de los clientes y que aprovechan debilidades de seguridad de los diferentes sistemas y aplicaciones, como por ejemplo los virus Blaster y Sasser.

Instalar software antivirus en el PC, el cual esté actualizado con las últimas firmas dadas por el fabricante respectivo.

RECOMENDACIONES DE SEGURIDAD GENERALES

Pornografía Infantil: Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

Control de virus y códigos maliciosos: Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).

Evite visitar páginas no confiables o instalar software de dudosa procedencia. La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta.

Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

Si sus programas o el trabajo que realiza en s computador no requieren de pop-up, Java support, ActiveX, Multimedua Autoplay o uto ejecución de programas, deshabilite estos.

Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

Control de phishing y sus modalidades:

- Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
- Para los sitios que indican ser seguros, revise su certificado SSL.
- Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

Robo de contraseñas:

- Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
- Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.
- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10 caracteres, combinada con números y caracteres especiales.
- No envié información de claves a través del correo u otro medio que no esté encríptado.

Correo electrónico:

- No publique su cuenta de correo en sitios no confiables.
- No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria. no debe contestarlo
- Nunca responda a un correo HTML con formularios embebidos
- Si ingresa la clave en un sitio no confiable. procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

Control de Spam y Hoax:

- Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del browser
- Para los sitios que indican ser seguros. revise su certificado SSL
- No reenvié los correos cadenas, esto evita congestiones en las redes y el correo. además el robo de información contenidos en los encabezados.

Control de la Ingeniería social:

- No divulgue información confidencial suya o de las personas que lo rodean.
- No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.
- Utilice los canales de comunicación adecuados para divulgar la información.

Firewall: A través de éste elemento de red se hace la primera protección perimetral en las redes de TV ISLA y sus clientes. Creando el primer control que reduce el nivel de impacto ante los riesgos de seguridad.

Antivirus: Tanto las estaciones de trabajo como los servidores de procesamiento interno de información en TV ISLA están protegidos a través de sistemas anti códigos maliciosos.

Antispam: Todos los servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los clientes, descongestionando los buzones y el tráfico en la red.

Filtrado de URLs: TV ISLA para el bloqueo de sitios con contenido de pornografía infantil, utiliza servidores para realizar el filtrado de estos sitios. El objetivo principal de este filtrado es denegar el acceso a los sitios que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales. Se sugiere instalar además sistemas parentales.

Seguridad a nivel del CPE: Los dispositivos de conexión final ubicados en las premisas de los clientes cuentan con elementos bases para la autenticación y autorización, con ello permiten hacer una conexión a Internet de manera más segura.