SEGURIDAD EN LA RED

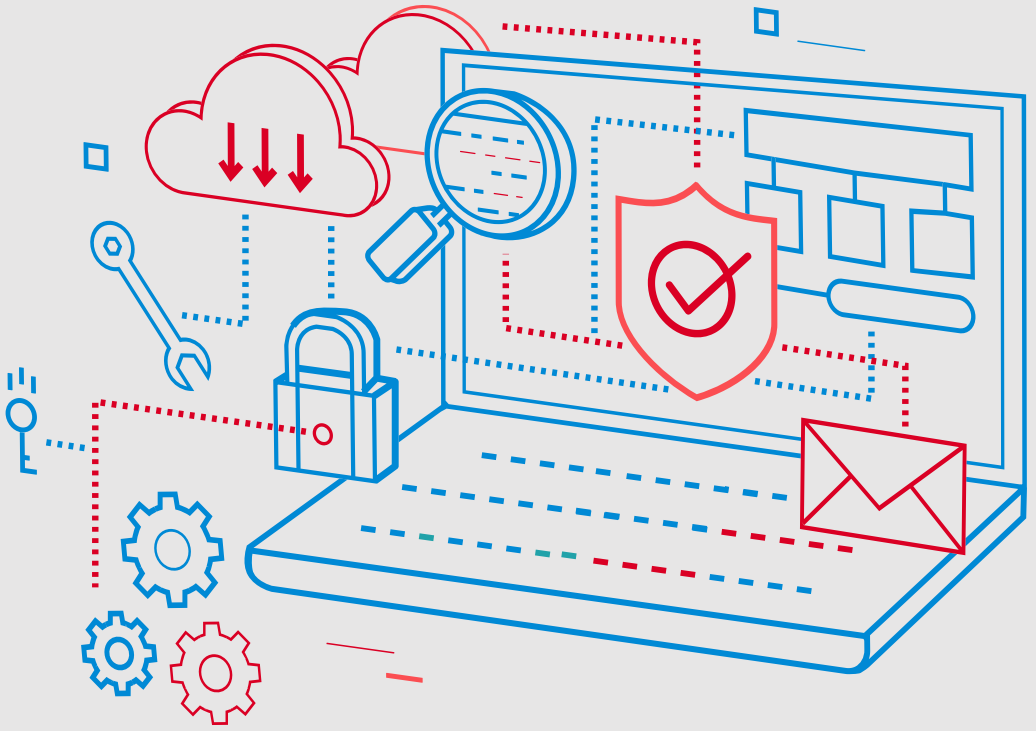
SOL
CABLE VISIÓN

Mecanismos de seguridad

SOL CABLE VISIÓN 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 SOL CABLE VISIÓN son protegidos a través de antivirus.

SOL CABLE VISIÓN 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.
SOL CABLE VISIÓN 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.



RIESGOS RELATIVOS A LA SEGURIDAD DE LA RED: FRAUDES

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.

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 solicita 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. Evite dar clic en links que vengan en los correos

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 esta.

Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

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.

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 mas común es hacerlo vía correo electrónico.

Normas básicas 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 mas 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 de 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.

¿Qué amenazas de seguridad son las más frecuentes en las organizaciones?

MALWARE

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.
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.

El malware que entra a través de los sistemas de correo, chat o sitios web es la amenaza más latente. Antiguamente nos referíamos solamente a virus, pero existe una fauna completa de malware que afecta la red:

• **Virus:** son programas que buscan infectar los ejecutables de los sistemas con la finalidad de replicarse a otros ejecutables. Los atacantes buscan cualquier forma que les permita lograr que un virus ingrese a un equipo y para ello se basa en correos o dispositivos removibles como pendrives que contienen virus a la espera de que el usuario lo ejecute.

• **Gusanos:** son virus que utilizan la red para replicarse. Es una forma mucho más rápida de propagación, pues aprovechan fallas de seguridad que no hayan sido actualizadas en las redes.

• **Caballos de Troya o troyanos:** son parecidos a los virus. El programa se presenta como una aplicación que hace algo útil para el usuario, el usuario lo baja y ejecuta a la espera de una funcionalidad, pero en realidad se trata de un virus que toma control del equipo y busca comprometer su funcionamiento, robar información o credenciales del usuario, o usa el equipo para enviar correos masivos (spam).

• **Spyware:** son programas que buscan información específica sobre el usuario: ancho de banda, a qué accede y a dónde, qué contiene su disco duro, etc., y normalmente es invisible. El impacto del spyware en una organización puede ser fatal, pues puede extraer información sensible de esta. Algunos intentan cambiar la funcionalidad del navegador. Es frecuente ver en equipos comprometidos con cierto tipo de malware que al intentar abrir un sitio web el spyware lo redireccione a otro. Un caso típico es el del spyware que redirecciona Google hacia otro buscador desconocido.

• **Adware:** es aparentemente inofensivo, pero envía anuncios a los usuarios con la finalidad de que hagan clic y su autor gane dinero por estos clics. El adware es muy común en softwares que se ofrecen gratuitamente, pero que en realidad buscan clics. Muchas veces el adware recolecta y envía información sobre el usuario del equipo, por lo que sí se convierte en un potencial peligro para la información que en él se almacene.

• **Ransomware:** es una aplicación maliciosa que infecta una computadora, cifrando ciertos archivos para restringir el acceso del usuario a estos, hasta que se pague un rescate a cambio de la clave para descifrarlos. Este tipo de malware se ha vuelto uno de los ataques más comunes en estos tiempos.

Estas no son las únicas amenazas de malware, hay muchas más. Y es importante hacer notar que muchas —sino todas— de estas amenazas se ven representadas no solamente en equipos de escritorio, sino además en los teléfonos inteligentes.

Era esperable que sucediera, pues al momento hay muchos más celulares inteligentes que equipos de escritorio y los atacantes siempre buscan el mercado que mayores réditos les genere. En este caso hay mayor posibilidad de ganancia en este nicho de equipos inteligentes por la gran cantidad de usuarios que los utilizan.

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.