Stealth Telecom del Ecuador S.A. como parte de su responsabilidad con los usuarios pone a su consideración recomendaciones para un uso seguro de los servicios de Internet y transmisión de datos.

Código malicioso: El código malicioso o malware es software diseñado para infiltrarse en una computadora sin el conocimiento de su dueño con el fin de robar, dañar o eliminar el software y la información almacenada, o aprovechar los recursos de la misma para efectuar otras acciones maliciosas.

Software espía o spyware: es un software que recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario con el propósito de conocer sus preferencias y enviarle publicidad relacionada con su perfil.

Phishing: es un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, haciendo uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.
Consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales suplantando la imagen de una empresa o entidad pública, se lo realiza habitualmente a través de mensajes de correo electrónico o de ventanas emergentes de forma que la posible víctima cree que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

sslStrip**:** es un ataque a nivel de usuario, que se presenta en los servidores web que utilizan el protocolo SSL para autenticar y cifrar comunicaciones entre navegadores y servidores Web.
Este ataque es capaz de crear un escenario creíble y engañar a los usuarios, quienes piensan que están trabajando en una página web segura, pero en realidad han sido redireccionados a otro computador atacante que se encuentra en la misma Red.

Spam: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor

Recomendaciones de Seguridad de Navegación en Internet

Utilice un navegador seguro.
Evite acceder a sitios desconocidos o no confiables.
No acepte la instalación automática de software.
No descargue archivos de sitios web no confiables.
Descargue los archivos en una carpeta y analícelos con un antivirus actualizado antes de abrirlos.
No ingrese información crítica o personal en formularios, páginas o foros.
Si un sitio requiere que ingrese información crítica o personal sólo hágalo en sitios seguros (la dirección debe comenzar por https).
Utilice un antivirus reconocido, verifique que siempre esté activo y actualizado a la fecha.
Analice siempre los medios removibles que se conecten a la computadora.

Ejecute un análisis completo (análisis en profundidad) del equipo periódicamente
No facilitar datos personales si no existe una completa seguridad sobre quién los va a recibir.
No facilitar más datos personales que los necesarios.
Comprobar los certificados de seguridad, en páginas que requieren datos personales.
Extremar la precaución en los archivos que reciben en sesiones de chat.
Actualizar los sistemas operativos y navegadores, con los parches que publican las firmas especializadas de software

Recomendaciones de Seguridad en Transacciones Económicas

Exigir siempre "conexiones seguras".
No introducir el número de la tarjeta en páginas de contenido sexual o pornográfico, en los que se solicita como pretexto, para comprobar la mayoría de edad.
No facilitar más datos personales de los necesarios.
Al enviar información, compruebe que, en la parte inferior del navegador Explorer, aparece un candado amarillo o un candado cerrado, en el caso de Mozilla. Esto indica que sus datos viajan encriptados.
Compruebe que los cargos recibidos se corresponden con los realizados.

Recomendaciones de Seguridad en el Correo Electrónico

No abrir mensajes de correo, de origen desconocido. Eliminarlo, directamente
No ejecutar ningún archivo adjunto que venga con mensajes sugerentes
Adopte las medidas necesarias, cuando le ofrecen "regalos" sustanciosos y, para recibirlos, tiene que llamar por teléfono a prefijos.
No facilitar la dirección electrónica con "demasiada" ligereza.
Tenga activado, constantemente, un antivirus
Visite páginas especializadas sobre seguridad informática.
Para que sus datos viajen seguros, envíe sus mensajes cifrados