



ELEMENTOS DE SEGURIDAD EN LA RED

INDICE

Conceptos generales de seguridad.....	1
Amenazas de seguridad.....	3
Fraudes.....	3
1. Telefónico: Dialers.....	3
2. Por Internet: Phishing.....	7
Internet Sano.....	8
TIP'S de Seguridad.....	9

ELEMENTOS DE SEGURIDAD

La red mundial Internet y sus elementos asociados son mecanismos ágiles que proveen una alta gama de posibilidades de comunicación, interacción y entretenimiento, tales como elementos de multimedia, foros, chat, correo, comunidades, bibliotecas virtuales entre otros que pueden ser accedidos por todo tipo de público. Sin embargo estos elementos deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos y potencializados a través del mismo servicio de Internet. UNE Telefónica de Pereira como proveedor del servicio de conectividad está convencido de que las relaciones con nuestros clientes se deben fortalecer desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y concejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet. Por esta razón ponemos a disposición de todos nuestros clientes y de la comunidad en general, conceptos teórico - prácticos que pueden evitar o reducir los riesgos a que se está expuesto cuando se interactúa con la Internet y sus elementos asociados.

Conceptos generales de seguridad

Confidencialidad:

Se refiere a que la información solo puede ser conocida por individuos autorizados

Integridad:

Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

Disponibilidad:

Se refiere a que la información pueda ser recuperada o esté disponible en el momento que se necesite.

Seguridad de la Información:

Son aquellas acciones que están encaminadas al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante un evento que las interrumpa.

Activo:

Recursos con los que cuenta la empresa y que tiene valor, pueden ser tangibles (servidores, desktop, equipos de comunicación) o intangibles (Información, políticas, normas, procedimientos)

Vulnerabilidad:

Exposición a un riesgo, fallo o hueco de seguridad detectado en algún programa o sistema informático.

Amenaza:

Cualquier situación o evento posible con potencial de daño, que pueda presentarse en un sistema.

Riesgo:

Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto.

Correo electrónico:

El correo electrónico es un servicio de red que permite que los usuarios envíen y reciban mensajes incluyendo textos, imágenes, videos, audio, programas, etc., mediante sistemas de comunicación electrónicos. Elementos de protección:

- **Firewall:** Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser Internet o una Intranet. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.
- **Anti-virus:** Programa capaz de detectar, controlar y eliminar virus informáticos y

algunos códigos maliciosos (Trojanos, Worms, Rootkits, Adware, Backdoor, entre otros).

- **Anti-spam:** Programas capaz de detectar, controlar y eliminar correos spam.
- **Criptografía:** Es el arte cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos.

Amenazas de seguridad

Phishing: Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada.

Se tienen dos variantes de esta amenaza:

- **Vishing:** Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).
- **Smishing:** Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

Spam: Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

Ingeniería social: Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesario para superar las barreras de seguridad.

Código Malicioso: Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Trojanos, Worms, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.

Hoax: Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.

Fraudes

1. Telefónico: Dialers

Existen programas que se instalan en el computador y que pueden incrementar su factura telefónica al solicitar llamadas de larga distancia no autorizadas por usted.

Estos programas conocidos como “dialers” o “marcadores telefónicos”, suelen ser

utilizados para redirigir, de forma maliciosa, las conexiones mientras el usuario navega en Internet. Su objetivo es finalizar la conexión telefónica que el usuario de Internet esté utilizando en ese momento (la que permite el acceso a Internet mediante el marcado de un determinado número de teléfono) y establecer otra marcando un número, la gran mayoría de veces, a otro país. Generalmente el usuario no se entera de estos cambios en la configuración hasta que le llega su factura telefónica con llamadas internacionales no solicitadas.

- ***¿Cómo funciona?***

Cuando nos conectamos a Internet a través de la línea telefónica, estamos implícitamente realizando una llamada telefónica a nuestro proveedor de Internet a través del módem de nuestro computador. El módem marca un cierto número de teléfono, que ha sido proporcionado por nuestro proveedor para configurar el acceso a Internet. El coste de realizar esta llamada a nuestro proveedor de acceso a Internet, lo conocemos ya que en el momento de la contratación del servicio lo elegimos nosotros.

El dialer aprovecha este mecanismo manipulando el número marcado y cambiando el del proveedor. Al cambiar la configuración de acceso, el computador marca a un proveedor de acceso a Internet en otro país.

Muchas veces el cliente no percibe esta modificación porque su navegación no se ve afectada, sin embargo está conectado y autenticado en otro proveedor diferente al que le vendió el servicio.

Generalmente, el ataque de un dialer se produce cuando se visitan determinadas páginas web, desde las que se descarga esta aplicación de forma oculta para él. El usuario puede o no darse cuenta. Algunos marcadores telefónicos deshabilitan el volumen del parlante para no delatarse cuando corta la llamada del proveedor de servicios predeterminado y activa la llamada del dialer no deseado. También pueden llegar a ocultar el icono de conexión.

- ***¿A quién le puede pasar?***

A cualquier usuario que tiene un computador e ingresa a Internet mediante el uso de líneas y módems convencionales a través de la Red Telefónica Pública o líneas RDSI (Red Digital de Servicios Integrados) que cuenten con los permisos necesarios de marcación a larga distancia internacional o cuando alguien va a su casa y utiliza su línea telefónica para navegar a través de la red. Los usuarios que se conectan a Internet por módem ADSL o cable módem no son susceptibles a los programas maliciosos de marcación, siempre y cuando el computador no tenga otra línea o derivación conectada a un módem convencional.

- ***¿Dónde está el peligro y cómo podemos ser víctimas?***

El peligro radica en que en la mayoría de los casos, la información ofrecida por las páginas web a los usuarios que navegan es escasa:

- No ofrecen términos y condiciones de uso claros o los ubican en lugares poco visibles, empleando otros idiomas, letra de tamaño muy reducido o colores que no facilitan su lectura.
- No se avisa de su instalación en la página que lo suministra.
- Saturan al usuario y únicamente insisten en que debe hacerse clic en <Sí> o <Aceptar> en determinada ventana emergente (pop up), esto como requisito para tener acceso a cierto contenido o para cargar el “visor de contenidos” que dicho en otras palabras, es el mismo programa dialer.
- En algunos casos extremos, se aprovechan de vulnerabilidades del navegador para instalarse en el sistema sin intervención del usuario.
- Hace una reconexión a Internet sin previo aviso, o lo intenta.
- No se informa del alto coste que va a suponer esa conexión.

Los dialers son descargados con autorización del usuario o de forma inadvertida al navegar en ciertas páginas de Internet. Estas páginas son por lo general las que ofrecen acceso a contenido gratuito de entretenimiento (juegos, canciones, imágenes, videos, etc.) así como programas sin licencia y contenido para adultos, pero cobran los mismos a razón del tiempo que estemos conectados a estos sitios.

Para usuarios inocentes, con mínimos conocimientos de informática e Internet puede suponer un serio problema porque estará realizando una llamada "especial" sin ser consciente de ello. Y además en posteriores conexiones (en los días sucesivos) podrá seguir siendo víctima porque el DIALER se queda instalado.

- ***¿Cuáles son las consecuencias?***

Entre las principales consecuencias para un usuario que puede tener instalado un dialers se destacan las siguientes:

- Factura telefónica con unas llamadas no autorizadas y por un alto valor.
- La creación de un nuevo acceso telefónico.
- La modificación del acceso telefónico a redes que el usuario utiliza habitualmente para sus conexiones de manera que, cada vez que sea ejecutado, el número marcado no sea el correspondiente al proveedor de servicios de Internet del usuario, sino el de un número internacional.
- Caídas frecuentes y repentinas en el acceso a Internet.
- Escuchar conversaciones o voces en otros idiomas.

- *¿Cómo puedo evitar que esto me suceda?*

Como la configuración del acceso a Internet es una actividad que se realiza sobre el computador personal, corresponde a cada uno de nosotros como usuarios establecer las medidas de protección más adecuadas. Estas son algunas:

- No dejar el módem del computador conectado a la red de telefonía básica si no va a navegar.
- No dejar el módem del computador conectado a la red de telefonía básica como respaldo cuando se tiene otro tipo de conexión.
- Fíjese en el número que marca su módem cuando aparece la ventana de conexión de acceso a Internet. Compruebe de manera periódica que el número a través del cual se va a hacer la conexión es realmente el contratado. Si requiere ayuda llame a su proveedor de internet.
- Sea precavido cuando navega en Internet y no acepte la instalación o descarga de archivos si desconoce su propósito.
- Desconfíe de la publicidad que ofrece 'absolutamente gratis' servicios que normalmente son de pago. Se recomienda que se extreme la precaución con la publicidad de páginas de contenido erótico, fondos de escritorio, salvapantallas, logos, melodías o casinos.
- No silencie el altavoz del módem, de esta forma puede monitorear la actividad del mismo y oír si se produce el marcado de un número nuevo mientras está conectado a Internet.
- Configure su navegador en el nivel más alto de seguridad que le sea permitido.
- Haga uso de la facilidad de código secreto ofrecida por su operador de telefonía local. Esto le permitirá activar y desactivar la restricción de llamadas de larga distancia desde su línea, así como llamadas hacia teléfonos móviles. Póngase en contacto con el operador de su línea telefónica para obtener mayor información sobre esta función.

Algunos de los tipos de dialers, no permiten ser desinstalados fácilmente o requieren de programas específicos para hacerlo, por esto:

- Haga uso de programas llamados Anti dialers, para bloquear marcadores telefónicos. Emplee uno que detecte y remueva posibles programas maliciosos que hayan podido instalarse sin su conocimiento. Para esto solicite la ayuda de un experto u obtenga mayor información sobre estos programas realizando una consulta en buscadores de Internet con la palabra clave “dialers” o “malware”, acompañado de las palabras “detectar”, “eliminar” o “remover”. Así mismo, consulte con su proveedor de Internet.
- Utilice herramientas de seguridad para proteger su computador.

2. Por Internet: Phishing


- **¿Cómo funciona?**

En primera instancia los atacantes crea un sitio Web similar al original, transcribiendo textos, pegando las mismas imágenes y los mismos formularios para digitar los datos. Una vez creado el sitio, lo publican en la Web con un alias parecido al sitio original.

Ej: Reemplazando un simple de caracteres, usando un dominio real como prefijo: Sitio oficial – www.sitioReal.com

- Sitio falsos:
www.sitioReal.com.sitio.com
- Variaciones:
 - www.sitioReal-account.com
 - www.sitioReal.actualiza.com
- Jugar con la percepción y la lectura del usuario:
 - www.sitio.Real.com
 - www.sitio.Real.com
 - www.sitio.Real.com/bin/actualiza

Adicional a esto, fijan una imagen simulando ser un sitio seguro (con certificados digitales) que a simple da mucha confianza pero son FALSOS:

Sitio Seguro 

Una vez realizado esta labor y utilizando spam, envían correos indicando a los “posibles” clientes o usuarios del portal a que actualicen sus datos, invocando la posibilidad de dar obsequios o premios si hacen esta acción.

- **¿A quién le puede pasar?**

A cualquier usuario que tenga un correo electrónico y acceso a Internet, donde periódicamente haga consultas y/o actualizaciones en portales que le presten servicios: Tiendas virtuales, Bancos, portal de correo, pago de servicios públicos, etc.

- **¿Dónde está el peligro y cómo podemos ser víctimas?**

El peligro radica en que, al ser una página falsa, inducen a los usuarios a que ingresen los datos personales, como cuantas de correo, número de tarjetas de crédito, claves, etc. y estos datos son recogidos por el atacante en bases de datos ajenas a las entidades oficiales de los sitios. Al sitio Web “similar” al original, es

difícil que el usuario se percate, en primera instancia, de que se trata de un engaño. Cuando llega un correo indicando sean actualizados los datos, los usuarios validan las bondades de estar actualizados e ingresan desde el enlace o link del correo, directamente a la página falsa. Al ser un spam “atractivo”, los usuarios hacen un reenvío de este a más usuario, formándose una cadena o Hoax para capturar más y más personas.

- ***¿Cuáles son las consecuencias?***

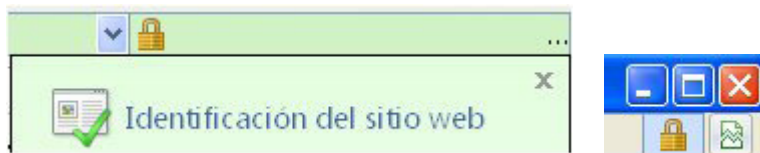
Una vez se ingresen los datos personales, son almacenados en bases de datos del atacante, que posteriormente utilizará en beneficio propio para realizar estafas o robos de dinero, dado que tiene en número de la cuenta bancaria y la clave de acceso (si el sitio falso es una entidad bancaria).

- ***¿Cómo se puede evitar?***

Siempre que llegue este tipo de mensajes, ingrese directamente al sitio oficial desde el browser o navegador, nunca desde el enlace o link enunciado en el correo, ni dando clic a dicho enlace.

Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo. Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si estén respaldados, de doble clic el icono de seguridad, que debe estar ubicado en la parte inferior derecha del navegador (no dentro de la página).

Ejemplo



Conozca de antemano cual es la dirección o URL del sitio real y valide este nombre cada que ingrese a realizar un proceso donde deba ingresar sus datos. Recuerde que el atacante utiliza técnicas que pueden engañar la percepción del sitio cuando se lee.

Si usted es un usuario frecuente de portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional (<http://www.policia.gov.co>), CAI virtual, los últimos eventos, recomendaciones y consultas en línea.

INTERNET SANO

Une – Telefónica de Pereira apoya las acciones para cumplir con las medidas impuestas por la Ley 679 de 2001 y el decreto 1524 de 2002, para la prevención y

detección de la pornografía infantil en Internet. Por esto, nos comprometemos a prevenir, bloquear, combatir y denunciar la explotación, alojamiento, uso, publicación, difusión de imágenes, textos, documentos, archivos audiovisuales, uso indebido de redes globales de información, o el establecimiento de vínculos telemáticos de cualquier clase, relacionados con material pornográfico o alusivo a actividades sexuales de menores de edad. Denuncie cualquier hecho que pueda catalogarse como pornografía infantil al Ministerio de Comunicaciones.

○ **Ministerio de Comunicaciones**

Teléfono: 01800 09 12667

Internet sano es la campaña del Ministerio de Comunicaciones para que todos los colombianos comprendamos el significado de la prevención de la pornografía infantil y juvenil en Internet.

Página Web: <http://www.internetsano.gov.co>

Otras entidades para hacer su denuncia: Dirección Central de Policía Judicial - DIJIN

○ **Grupo Investigativo Delitos Informáticos**

Carrera 77A # 45-61 Barrio Modelia -
Bogota D.C.

Telefonos: PBX: 4266301-4266302

Dirección de correo: adepegridi@dijin.policia.gov.co

<http://www.delitosinformaticos.gov.co/joomla/>

○ **Fiscalía General de la Nación:**

Teléfono: 01800 09 12280

Página web: <http://www.fiscalia.gov.co>

e-mail: contacto@fiscalia.gov.co

TIP'S DE SEGURIDAD

Pornografía Infantil:

Evite Alojar, publicar o transmitir 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 su computador no requieren de pop-up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos.
- Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

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 reenvíe 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.

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 8 caracteres, combinada con números y caracteres especiales.
- No envíe información de claves a través del correo u otro medio que no esté encriptado.

Código Secreto: (En su servicio de telefonía)

- Con el servicio de código secreto los usuarios de Une-Telefónica de Pereira pueden controlar sus llamadas de forma segura en su hogar. Este sistema permite a través de una clave bloquear y desbloquear el acceso al servicio de Larga Distancia Nacional e Internacional (directas o con operadora), llamadas a celulares y número 901.
- Ventajas y Beneficios:
 - ✓ Controlar que se realicen llamadas diferentes a las locales
 - ✓ Prevenir el uso indebido de líneas telefónicas
 - ✓ Facilidad para cambiar la clave de seguridad cuando se requiera
- Recomendaciones:
 - ✓ Cambiar la clave periódicamente
 - ✓ Recordar bloquear el teléfono después de realizar una llamada con destino diferente a local
 - ✓ No revelar la clave del Código Secreto a personas ajenas al hogar

UNE – Telefónica de Pereira piensa en su seguridad

Por esto, le sugiere no responder ningún correo donde se solicite información privada, confidencial, datos bancarios, entre otros, ya que podría tratarse de un intento de fraude hacia usted.