CIBERSEGURIDAD

SCP

Privacidad de los datos

Parte II

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

open source

Índice

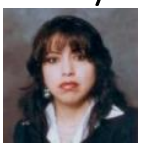
“Si no actuamos ahora en resguardar nuestra privacidad, todos nos volveremos victimas de robos de identidad”

— Bill Nelson —

CRÉDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

SCProgress

www.scprogress.com

Facebook

Twitter

Robo de identidad en línea

En nuestra revista anterior, resaltamos la importancia de proteger nuestros datos personales al realizar nuestras actividades en línea, así como, la forma en la que vamos dejando nuestra huella digital en las diferentes dinámicas en operan en el Internet.

En esta ocasión para completar nuestra emisión sobre la privacidad de los datos, tocaremos diferentes temas, entre los cuales se encuentra el robo de nuestra identidad en línea.

Para ello tendremos que definir desde ciertos conceptos básicos del robo de identidad o usurpación de identidad, que es la apropiación de la identidad de una persona, es decir, hacerse pasar por otra persona, asumir su identidad ante otras personas en público o en privado, en general, para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona.

Por otro lado, el robo de identidad también es utilizado con el fin de perjudicar a una persona, difamarlo o manchar su nombre con diversos fines que el criminal busque.

El caso más común hoy en día se da cuando un atacante, por medios informáticos o personales, obtiene su información personal y la utiliza ilegalmente.

"El uso de Internet, el desarrollo de las

tecnologías digitales y la emoción causada por las redes sociales, forman parte de nuestra vida cotidiana. Si bien estas herramientas facilitan nuestras transacciones e intercambios, también pueden escapar a nuestro control y generar nuevos riesgos". Con estas palabras, el grupo LegisDigit lanzó una campaña para generar conciencia sobre la privacidad de los datos a la hora de protegerlos en Internet.

El grupo LegisDigit, realizó un pequeño experimento para demostrar lo sencillo que es hacer caer a las víctimas. En un puesto en medio de la calle invitaban a un concurso para ganar un iPad, con solo iniciar sesión en Facebook en el terminal que estaba disponible para los transeúntes. Una vez completado el proceso, se le pedía al participante que mirara hacia atrás, y que viera como en las pantallas aledañas empezaban a aparecer las imágenes de Facebook del usuario que sin muchos reparos inició sesión en la red social.

"*Tu identidad digital se puede robar más fácilmente de lo que crees*", es la moraleja de la historia que leyeron -en alemán- los que cayeron en la inocente, pero preocupante jugada. Seguramente varios de los afectados ahora se van a pensar dos veces al momento de abrir su Facebook por cualquier parte.

El robo de identidad es el delito de más rápido crecimiento en el mundo. Hasta no hace mucho tiempo, cuando un ladrón robaba la billetera o porta documentos, el dinero era lo único que pretendía. Con el tiempo, los datos de los documentos de identidad como, por ejemplo, la tarjeta de crédito, la tarjeta de débito, los cheques y cualquier otro documento que contenga los datos personales se han vuelto muy importantes.

En el transcurso de cualquier día, esta información se divulga al hacer transacciones en persona, por teléfono y online para efectuar la compra de productos y servicios. Si esta información confidencial cae en manos de un delincuente, podría utilizarse para robar la identidad financiera y realizar muchas de las actividades en nombre del titular.

Nadie está a salvo de este delito ni puede tenerse la certeza de que nunca ocurrirá. Lo importante es conocer los métodos existentes para reducir las probabilidades de que ocurra y las medidas a tomar en caso de que suceda.

Lamentablemente, la mayoría de las personas no se enteran que han sido víctimas de robo de identidad hasta que solicitan un crédito y se los niegan, quieren contratar el servicio de telefonía celular y no pueden y en la mayoría de los casos, cuando aparecen cobros sospechosos en los resúmenes de las tarjetas de crédito.

Existen varios métodos para obtener datos de la información personal:

- **Correos falsos**: este es de los más comunes. La gente abre cuentas al por mayor con nombres falsos y empieza a enviar datos o a amenazar a

gente con tu nombre. La gente agredida denunciará tu nombre aunque tú no estés involucrado.

- **Personal**: cualquier persona maliciosa podría obtener información que escuchó o vio de parte suya que le garantice acceso a algún recurso valioso.
- **Ataque organizado**: cualquier atacante podría intentar superar la seguridad de un banco, empresa u organización para obtener información personal de los clientes para luego acceder a algún recurso de esa empresa.
- **Ataque a servidores de almacenamiento de información online**: el atacante puede tratar de obtener datos de un servidor de almacenamiento de datos en la nube; obteniendo contraseñas, número de cédula de identidad, cuentas bancarias, etc.
- **Redes sociales**: Se han empezado a recibir denuncias de extorsión que se hacen mediante la creación de perfiles falsos en las redes sociales. La gente empatiza contigo, sabe tus datos personales y luego te extorsiona con ellos. Ten cuidado de qué información subes a la red y a quien conectas en tus redes sociales.
- **Compras con tu perfil**: En la medida en que los teléfonos inteligentes se hacen más populares y el uso de aplicaciones están a la orden del día, se suele dejar abiertas las sesiones de las aplicaciones en nuestro teléfono, si lo roban o lo dejas sin vigilancia, alguien puede meterse a comprar mediante tu perfil y datos personales y luego tú serás el sorprendido cuándo te lleguen los estados de cuenta con cargos que tú no hiciste desde tu teléfono.
- **Phishing**: este tipo de robo de identidad es el más común y peligroso, se suele hacer a través de correos electrónicos en los que piden que se haga clic a un enlace malicioso, o se descargue un archivo infectado o se envíen datos personales a un destinario que no es quien dice ser. Así también, crean sitios web que se hacen pasar por un sitio legítimo, como un banco, copiando su apariencia como su contenido, para que la víctima intente acceder a sus cuentas y así revele sus datos de acceso a los delincuentes.

Las víctimas de estos delitos no son siempre personas físicas, también pueden ser empresas, como páginas web que se hacen pasar por una empresa en particular para publicar información negativa que dañe su reputación y les haga perder clientes.

Es importante que tanto profesionales como empresas y marcas conozcan cuál es la información que aparece sobre ellos en Internet, mediante un informe de presencia online, y así detectar posibles robos de identidad de internet, infracciones de propiedad intelectual o abusos de marca.

Tampoco hay que olvidar que cualquiera puede ser víctima de estos delitos, tanto por la vía de los ataques informáticos (explotación de vulnerabilidades en programas, malware, etc.) como por la vía de la ingeniería social (aprovechándose de los fallos humanos, de la buena fe, la ingenuidad la imprudencia o la falta de atención a las personas). Además, la situación será más grave si afecta a personas vulnerables

(menores de edad, discapacitados, etc.) o si la repercusión es muy alta (por ejemplo, no es lo mismo que una foto la vean 10 personas a través de un mensaje privado, que esté colgada en un sitio web que visitan 100.000 personas al día, tampoco es lo mismo que esté accesible durante unos días o durante meses o años).

Es un hecho que no hay seguridad que valga, solo basta un buen señuelo, para que caigamos en la trampa. Por lo tanto es imprescindible tener mucho cuidado de donde se conectan, a quien le prestan sus equipos y a las falsas propagandas que les puedan ofrecer (no todo lo que brilla es oro).

También es importante recordar que siempre debemos mantener nuestros equipos informáticos, con software de antivirus actualizado, y contar con la prevención adecuada para la detección de infiltraciones.

Avira, es desarrollado en el concepto Alemán de calidad, no produce molestias al cliente y el altamente eficiente, previniendo amenazas en tiempo real, con detección basada en firmas, examen heurístico y análisis basado en la nube que ofrece una protección completa frente a los programas maliciosos.

Avira, también brinda protección completa en el momento del acceso, su tecnología en la nube en tiempo real protege los procesos en ejecución, el acceso a los archivos y la memoria del sistema frente al spyware, rootkits y otros tipos de programas maliciosos ocultos.

Si quieres conocer más sobre Avira, visita la página web www.scprogress.com, o escribe directamente a avira@scprogress.com, personal técnico altamente calificado de **SCProgress**, te ayudará con la mejor opción de acuerdo a tus requerimientos o los de tu empresa.

FUENTES:

- https://es.wikipedia.org/wiki/Robo_de_identidad
- https://www.mundoxat.com/foro/showthread.php?24234-As%C3%AD-de-f%C3%A1cil-se-puede-robar-tu-identidad-en-internet
- https://www.certsuperior.com/Blog/7-maneras-de-robar-la-identidad-de-alguien-en-internet
- http://www.seguridad.unam.mx/documento/?id=16
- http://www.voluntaddigital.com/suplantacion-de-identidad-y-delitos-en-internet/
- http://www.dinero.com/empresas/articulo/riesgo-online-robo-identidad/173291

Capacitación en Ciberseguridad y Antimalware

"La necesidad de capacitación surge por la diferencia entre lo que uno debería saber y lo que sabe realmente"

El personal responsable de las áreas de sistemas, así como los usuarios, deben conocer sobre la infinidad de ataques informáticos amenazas, ataques a la información y a las infraestructuras tecnológicas, los mantienen como áreas vulnerables permanentes, facilitando las actividades fraudulentas de hackers, quienes han visto como un gran negocio lucrativo, la sustracción de datos, ya sea personal, financiera, confidencial, etc.

La capacitación en seguridad informática, se vuelve relevante e importante para evitar que las empresas e instituciones, se vean afectadas ante este tipo de amenazas.

SCProgress cuenta con asesores altamente especializados a nivel internacional, lo que nos permite brindar cursos de capacitación en diversos temas tecnológicos, especialmente en el área de seguridad informática, su amplia experiencia y conocimientos, les ha permitido participar en eventos nacionales e internacionales como la conferencia organizada por la CEPOL Research & Science Conference (Organismo acreditado de la Unión Europea), realizada en Budapest el año 2016.

En esta ocasión SCProgress, consiente de la importancia que prestan las instituciones a la seguridad de la información, y ante el incontrolable crecimiento de las amenazas, ha organizado y pone a disposición de sus lectores y clientes, capacitación en los siguientes temas:

Certificación en Ciberseguridad de la RED	Introducción al análisis y comportamiento del malware
Contenido: • Fundamentos de red de computadoras y defensa • Amenazas, vulnerabilidades y ataques a la red • Controles, protocolos y equipos para la seguridad de la red Diseño e implementación de políticas de seguridad en la red • Seguridades físicas • Seguridades en los Host • Configuración y administración segura de Firewalls • Configuración y administración segura de IDS • Configuración y administración segura de VPNs • Protección de redes inalámbricas • Monitoreo y análisis del tráfico de la red • Gestión de riesgos y vulnerabilidades • Data backup y recuperación de datos • Respuesta y manejo de incidentes	**Contenido:** • Análisis de malware • Indicadores de infección • Malware signatures • Categorías de malware • Mass vs Targeted malware • Metodología de análisis de malware • Herramientas Antimalware • Malware empaquetado y oculto • DLL Hijacking • Magic labels • Formatos de archivos • Dynamic Link Libraries • Detección de virtualización de malware • Dependency Tracing • Modificación de registros • Manipulación de archivos del sistema • Análisis de tráfico de la red • Sandboxes

Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: **www.scprogress.com**, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

Legislación ecuatoriana para el robo de identidad en línea

Como hemos indicado en el artículo anterior, absolutamente ninguna persona se encuentra totalmente segura frente al robo de identidad, sobre todo, considerando que la tecnología crece día a día, así como también los atacantes mejoran sus estrategias para sustraer los datos y hacer mal uso de los mismos.

En el Ecuador, actualmente existen sanciones para este tipo de delitos estipulados en el Código Orgánico Integral Penal (COIP), vigente desde el 10 de agosto del 2014, en el cual contempla y sanciona los delitos informáticos como por ejemplo: la revelación ilegal de base de datos, la interceptación ilegal de datos, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos y los accesos no consentidos a un sistema telemático o de telecomunicaciones, la pornografía infantil, el acoso sexual.

Con la finalidad de dar continuidad a la presente edición y para conocimiento de nuestros lectores, redactamos textualmente los artículos del COIP, dónde se tipifican la apropiación fraudulenta de información a través de medios informáticos, relacionada con la privacidad de los datos:

"En la Sección Sexta del COIP, delitos contra el derecho a la intimidad personal y familiar, Artículo. 178: Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

En la Sección Novena del COIP, delitos contra el derecho a la propiedad, Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio

suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes".

Si bien es cierto en nuestro país, existen sanciones para los delitos informáticos, también es evidente que necesitamos hacerlas más drásticas, y ampliar más los tipos de delitos informáticos con relación al robo de identidad en línea, para prevenir y disminuir ser víctimas de personas mal intencionadas que lo único que buscan es perjudicar y aprovecharse de personas que de manera ingenua o por descuido son afectadas.

Si hemos sido víctimas de este tipo de delincuencia, debemos acercarnos a realizar la denuncia en los servicios de Atención Ciudadana de la Fiscalía más cercana a nuestro lugar de residencia.

Para **SCProgress**, es importante conocer su sentir con respecto a este tema, por lo que invitamos a nuestros lectores y seguidores, a que nos envíen sus opiniones, al nuestro correo electrónico ciberseguridad@scprogress.com, las mismas que serán publicadas en nuestra nueva sección de opinión, en la siguiente edición.

¿Cómo evitar el robo de identidad?

Como hemos venido indicando en los artículos y ediciones de nuestras revistas, los piratas informáticos tienen muchas formas de robar información personal y dinero. Es imposible que podamos dar las llaves de nuestros domicilios a un ladrón, por lo tanto es primordial protegerse contra el fraude y el robo de identidad en línea.

SCProgress realiza una recopilación de los trucos comunes que los piratas emplean, para que puedas protegerte del fraude en línea y del robo de identidad:

No responda si ve un mensaje de correo electrónico sospechoso, un mensaje instantáneo o una página web que solicita tu información personal o financiera.

Siempre tenga cuidado con los mensajes o sitios que piden su información personal o los mensajes que dirigen a una página web desconocida que pide cualquiera de los siguientes datos:

- Nombres de usuario.
- Contraseñas
- Números de seguridad social
- Números de cuentas bancarias
- PIN (números de identificación personal)
- Números completos de tarjetas de crédito
- Apellido de soltera de tu madre
- Su fecha de nacimiento

No llene ningún formulario o pantalla de acceso que pueda provenir de esos mensajes. Si alguien sospechoso pide que llene un formulario con sus datos personales, no sienta la tentación de empezar a llenarlo. Aun si no presionas el botón "Enviar", podría estar enviando información a los ladrones de identidad con solo llenar sus datos en los formularios.

Si aparece un mensaje de alguien que conoce, pero no parece de él, puede ser que su cuenta haya sido vulnerada por un pirata informático que está tratando de obtener dinero o información de su parte, así que tenga cuidado con lo que responde. Las tácticas comunes incluyen el pedido de dinero urgente con la excusa de que está perdido en otro país o diciendo que le robaron el teléfono, por lo que no se lo puede llamar. El mensaje también puede pedir que haga clic en un vínculo para ver una foto, un artículo o un video, que en realidad le lleva a un sitio que podría robarle información, por lo que debe pensar antes de hacer clic.

Elimine los correos spam que le soliciten información personal y mantenga actualizados su software antivirus y antispyware y sobre todo nunca envíe por correo electrónico los números de sus tarjetas de crédito.

Nunca ingrese su contraseña cuando llegue a un sitio mediante un vínculo en un correo electrónico o un chat en el que no confía.

Incluso si piensa que es un sitio de confianza, como su banco, es mejor ir directamente al sitio mediante el uso de un marcador o escribiendo la dirección del sitio directamente en el navegador.

No envíe su contraseña por correo electrónico ni la comparta con otros.

Las contraseñas son las llaves a sus cuentas y servicios en línea y, al igual que en la vida real, debe tener cuidado con la persona a quien le da las llaves. Los sitios y servicios legítimos no piden que envíe sus contraseñas por correo electrónico, por lo que no debe responder a las peticiones de contraseñas para sitios en línea.

Debido a que las contraseñas son tan importantes, debe pensar cuidadosamente antes de tomar la decisión de compartirlas con los demás, incluso amigos y familiares. Al compartir las contraseñas, existe un mayor riesgo de que alguien pueda abusar de sus cuentas, ingresando información que no desea ingresar o utilizando la cuenta de manera que no aprueba. Por ejemplo, si comparte su contraseña de correo electrónico con alguien, esa persona puede leer sus correos electrónicos personales, tratar de usar su cuenta de correo electrónico para acceder a otros servicios en línea que utiliza, como el banco o los sitios sociales, o usar su cuenta para hacerse pasar por usted. Por último, cuando comparta la contraseña con alguien, tendrá que confiar en ellos para que esté segura, ya que pueden compartirla con los demás intencionadamente o

por accidente.

Preste mucha atención cuando se le pide que acceda en línea.

Busque señales que indiquen su conexión con el sitio web.

En primer lugar, mire la barra de direcciones de su navegador para ver si la URL parece real. Realice sus compras en línea sólo en sitios web seguros (verifique que en la parte inferior del navegador aparezca el ícono de un candado cerrado.

También debe verificar si la dirección web comienza con https://, lo que indica que la conexión al sitio web está encriptada y cuenta con una mayor protección contra intromisiones o interferencias. Algunos navegadores también incluyen un ícono de candado en la barra de direcciones junto a https:// para indicar claramente que la conexión está encriptada y que está conectado de forma más segura.

Denuncia trampas y correos electrónicos sospechosos.

La mayoría de los proveedores de correo electrónico, le permiten hacer esto. Si denuncia un mensaje sospechoso en Gmail, Hotmail, Yahoo, por ejemplo, ayudará a bloquear a ese usuario para que no le envíe más mensajes de correo electrónico y permitirá que los operadores detengan ataques similares.

No olvidar normas básicas cuando nos encontramos en Internet.

- Antes de aceptar cualquier tipo de servicio, debemos leer los detalles sus términos y condiciones con el fin de saber dónde se almacenan nuestros datos, con quien podrían ser compartidos o las medidas de seguridad implementadas para protegerlos.
- Por supuesto, verifica la legitimidad de la empresa accediendo a ella desde otra ventana del navegador y buscando información en la propia red.
- Recuerda que todo aquello que compartes en internet constituye tu huella digital, es decir, algo así como tu vida reflejada en internet. Por tanto, debes ser prudente a la hora de compartir cierto tipo de contenidos, especialmente imágenes que te podrían comprometer y que podrían ser utilizadas por ciberdelincuentes para dañar tu imagen, hacerte chantaje, etcétera.
- ¡Cuidado con las redes WiFi a las que te conectas! En la actualidad prácticamente cualquier tienda, cafetería, centro comercial, etcétera ofrece conexión WiFi a sus clientes pero, ¿son seguras estas redes? En la mayoría de los casos no, de tal forma que a través de ella, cualquier ciberdelincuente podría accedes a tu dispositivo robando tus datos personales, de acceso a redes sociales, mensajes, números de teléfono, direcciones de correo, datos bancarios y de tarjetas de crédito y débito, y el incluso tomando el control del terminal.
- En aquellas redes sociales donde compartas información personal, como Facebook, asegúrate de incluir como amigos a quienes realmente lo son, personas que conoces, o empresas reales y seguras, pero no a cualquiera que lo solicite y del cual desconoces sus intenciones. Por otro lado, procura configurar la visibilidad de tu perfil sólo para aquellas personas incluidas como amigos o contactos, no dejes tu perfil abierto a cualquiera.

Y para el final dejamos la norma más básica y elemental de todas: utiliza contraseñas seguras. Por favor, no cometas el error de utilizar como password tu fecha de nacimiento, ni secuencias sencillas como “123456” ni nada relativo a tu información personal. Este tipo de contraseñas son extremadamente débiles y fáciles de descubrir por cualquier programa utilizado para ello. Nuestro consejo: que tu contraseña incluya números, letras mayúsculas, letras minúsculas y, si el servicio lo permite, también algún símbolo como asteriscos, una barra inclinada, guión, etcétera.

FUENTES:

- https://www.google.com/intl/es-419/safetycenter/everyone/cybercrime/identity-theft/
- http://mexico.smetoolkit.org/mexico/es/content/es/8127/C%C3%B3mo-protegerse-contra-el-robo-de-identidad

¿Qué es el cyberstalking y cómo evitarlo?

La tecnología y el uso del Internet nos ha llevado a vivir en la era de las transacciones en línea, a hacer amigos en diferentes partes del mundo sin tener que movernos de nuestros hogares, y un sin número de actividades realizadas a través de nuestros computadores o dispositivos móviles. Pero también tiene una parte negativa de todo ello, es que esta misma tecnología también ha abierto el camino para que ciertas personas lleven a cabo malas acciones.

En la actualidad se hablan de nuevos delitos, a los que también se les asignan nombres, que en muy pocas ocasiones los escuchamos y la mayoría de veces las dejamos pasar por alto, o no le prestamos la atención debida. Uno de los nuevos términos de los ciberdelitos es: Cyberstalker.

SCProgres siempre pendiente por alertar a nuestros lectores sobre las nuevas amenazas, así como, las existentes, ha realizado la recopilación de información, para darles a conocer sobre qué es el cyberstalking y como evitarlo.

Definición del cyberstalking.

El cyberstalking es, básicamente, acoso online. Se ha definido como el uso de tecnología, en particular Internet, para acosar a una persona. Algunas de las características comunes son: acusaciones falsas, seguimiento, amenazas, robo de identidad y destrucción o manipulación de datos. El cyberstalking también incluye la explotación de menores, ya sea sexual o de otro tipo.

El acoso puede adoptar muchas formas, pero el denominador común es que no es deseado, es a menudo obsesivo y, por lo general, ilegal. Los acosadores cibernéticos utilizan el correo electrónico, los mensajes instantáneos, las llamadas telefónicas y otro tipo de dispositivos de comunicación para cometer acoso, el cual puede manifestarse como acoso sexual, contacto inadecuado o, simplemente, una forma de molesta atención a su vida y las actividades de su familia.

Los niños utilizan el término "acoso" para describir las actividades de una persona mediante su red social. Es importante que no le restemos importancia a la preocupante naturaleza del cyberstalking empleando el término de manera incorrecta. Un nuevo anuncio de televisión en la ciudad de México de un destacado proveedor de telefonía móvil muestra a una joven espiando a su novio a través de la ventana del dormitorio y supervisando las actividades online realizadas por él desde su teléfono móvil. Si bien está pensado como un anuncio publicitario con humor, resulta muy perturbador cuando el acoso sucede en el mundo real.

Es interesante que este mismo anuncio ponga en evidencia un importante factor sobre el cyberstalking: generalmente, no lo comete un extraño, sino alguien que usted conoce. Puede tratarse de un ex, un antiguo amigo o alguien que simplemente desea molestarle a usted y a su familia de un modo inadecuado.

Cómo daña el cyberstalking?

Nadie debe tomar a la ligera el acoso cibernético. Si la idea de que alguien nos esté acechando en Internet y recopilando nuestra información personal nos da miedo, entonces hay que ser conscientes del acoso cibernético y estar alerta en el Internet con el fin de evitar cualquier contratiempo.

El cyberstalking puede dar mucho miedo. Es capaz de destruir amistades, méritos, carreras, además de la autoestima y la seguridad en uno mismo. En última instancia, puede exponer a la víctima a un peligro físico aún mayor cuando el acoso también se produce en el mundo real. Sí, estamos hablando de algo serio. Las víctimas de violencia doméstica suelen ser víctimas del cyberstalking. Deben ser conscientes, al igual que el resto de las personas, de que la tecnología puede facilitar el cyberstalking. Un programa spyware puede utilizarse para supervisar todo lo que ocurre en su ordenador o teléfono móvil, y otorgar un inmenso poder y volumen de información a los acosadores cibernéticos.

Consejos anti-acoso

A continuación se indican algunas sugerencias importantes para ayudarle a evitar el cyberstalking, ya sea que esté dirigido a usted, a su equipo informático o su familia:

Vigile el acceso físico a su computador y a otros dispositivos habilitados para usar Internet, como teléfonos móviles. Los acosadores cibernéticos utilizan dispositivos de software y hardware (a veces adosados a la parte trasera de su PC sin que usted lo sepa) para supervisar a sus víctimas.

Siempre asegúrese de cerrar la sesión de los programas cuando se aleje del ordenador o utilice un salvapantallas con una contraseña. La misma sugerencia se aplica a las contraseñas de los teléfonos móviles. Tanto sus hijos como su pareja deberían seguir los mismos buenos hábitos.

Asegúrese de poner en práctica una buena gestión y seguridad de las contraseñas. Nunca divulgue sus contraseñas. Y asegúrese de cambiarlas con frecuencia. Esto es muy importante.

Cada cierto tiempo, realice una búsqueda online de su nombre o el de los miembros de su familia para saber qué información sobre usted y sus hijos está disponible online. No dude en buscar en las redes sociales (incluso en las de sus amigos y colegas) y asegúrese de eliminar cualquier contenido privado o inadecuado.

Elimine o configure como privados todos los calendarios o itinerarios online (incluso en su red social) en los que mencione las actividades en las que planea participar. Dichas actividades podrían indicarle al acosador dónde va a estar y cuándo.

Utilice la configuración de privacidad en todas sus cuentas online para limitar la información que comparte online con quienes no forman parte de su círculo de confianza. Puede utilizar esta configuración para evitar que su perfil aparezca cuando alguien realiza una búsqueda con su nombre. También puede impedir que otras personas vean sus mensajes y fotos.

Si sospecha que alguien está utilizando un programa spyware para hacer un seguimiento de sus actividades diarias y considera que está en peligro, use únicamente computadores o teléfonos públicos para solicitar ayuda. De lo contrario, el acosador cibernético sabrá acerca de su intento de obtener ayuda, lo que podría exponerle a un peligro aún mayor.

Como siempre, utilice un software de seguridad de calidad y actualizado para evitar que alguien introduzca spyware en su ordenador mediante un ataque de phishing o una página web infectada. El antivirus Avira, es la mejor opción para la protección de sus equipos, ya lo hace en tiempo real, previniendo cualquier tipo de infiltración ya sea por spyware o malware, disminuyendo drásticamente las probabilidades de sufrir un acoso.

Enseñe a sus hijos

Es posible que parezca un disco rayado, pero repítales a sus hijos que nunca deben divulgar información personal online, sin importar lo

seguro que les parezca. Dígales que nunca revelen su nombre verdadero, la escuela, la dirección, ni la ciudad en la que viven. Los números de teléfono no deben difundirse online, y en caso de que un extraño contacte con ellos por cualquier medio, deben comunicárselo a usted inmediatamente. Haga que sus hijos le informen si están sufriendo un acoso cibernético. Como madre o padre, debe informar sobre el cyberstalking a un maestro o una autoridad de la escuela, y, si parece un asunto serio, debe denunciarlo ante la policía.

Denúncielo!

Si está sufriendo un acoso cibernético, recuerde guardar una copia de todos los mensajes o las imágenes online que puedan utilizarse como prueba. De hecho, enseñe a sus hijos cómo utilizar la función "imprimir pantalla" u otras funciones del teclado para guardar capturas de pantalla.

Lo más importante es que no tema denunciar el cyberstalking ante la policía. En nuestro país, ya se receptan este tipo de denuncias, ya que son consideradas como un delito.

FUENTES:

- http://www.prucommercialre.com/que-es-el-acoso-cibernetico/
- http://www.fiebrelatina.co/tecnologia/nueve-maneras-de-protegerse-de-cyberstalking
- https://mx.norton.com/cyberstalking/article
- https://www.mundoxat.com/foro/showthread.php?24234-As%C3%AD-de-f%C3%A1cil-se-puede-robar-tu-identidad-en-internet

Cyberoam®

Rincón de los expertos

¡Los 10 consejos más importantes para proteger tu identidad online!!!

Considere que cada tres segundos es robada una identidad en algún lugar en el mundo. ¿Reflexione cuál es su riesgo de ser el próximo?

1. Excluya información personal importante de sus perfiles en las redes sociales.
2. Verifique frecuentemente sus políticas de seguridad en las redes sociales.
3. Use contraseñas fuertes en todos los medios online que utilice.
4. Utilice diferentes contraseñas en cada uno de los medios tecnológicos y redes sociales que disponga, puede gestionar todos ellos a través de aplicativos como Avira Vault.
5. Mantenga desactivadas las opciones de GPS en todos los celulares y dispositivos móviles, para garantizar su privacidad.
6. Mantenga todas sus conexiones seguras, implemente VPNs.
7. Evite leer correos desconocidos o aceptar invitaciones en las redes sociales de personas que no conoce.
8. Antes de ingresar a cualquier sitio web, verifique que este activado el protocolo SSL, utilice únicamente https://, recuerde la '**s**' es importante.
9. Verifique constantemente el estado de su banca online, y los gastos que en ella se realiza.
10. Sea prudente con ofertas o cualquier otra actividad sospechosa que encuentre en sus correos o redes sociales, como premios, prestamos pre-aprobados, etc.

Recuerde siempre estos consejos por su seguridad y la de su familia.

Novedades

Ganador de entradas para acompañar a nuestra selección en el partido Ecuador Vs. Colombia

SCProgress apoyando a la selección del Ecuador, así como, premiando a nuestros clientes y seguidores, realizó una encuesta de conocimientos, para obsequiar dos entradas totalmente gratis, al partido de futbol en contra de nuestros vecinos colombianos, para quien haya obtenido la mejor puntuación.

El ganador fue el señor Paulo Abadiano, quien pudo asistir y apoyar junto a un acompañante, a la TRI en tan importante juego.

Queremos agradecer la participación de todos, e invitarlos a que nos sigan en nuestras redes sociales: Facebook, twitter y nuestra página web www.scprogress.com, seguiremos premiando su confianza a nuestros productos y servicios.

A continuación ponemos en su conocimiento la encuesta realizada, junto con las respuestas.

1.- Cuáles son los módulos de Internet Protection de AVIRA?

Firewall, Mail Protection, Web Protection

2.- Cuáles son las 3 áreas que existen de red?

- LAN
- WAN
- MAN

3.- Cuál es la velocidad máxima que se puede alcanzar con cable CAT6?

1 Gbps

4.- Cuáles son los medios de transmisión de red?

- Cobre
- Fibra Óptica
- Wireless

5.- En que frecuencias trabajan las redes inalámbricas WiFi?

2.4 GHz y 5 GHz

6.- Qué diferencia hay entre un Dominio y un Grupo de Trabajo en Redes?

Grupo de trabajo: Es un grupo de ordenadores que se encuentran conectados a uno y comparten impresoras u otros dispositivos.
Dominio: Es una agrupación de ordenadores en torno a un servidor centralizado que guarda la lista de usuarios y nivel de acceso de cada uno.

7.- Cuántas direcciones y hosts validos obtenemos en una red con mascara 19.

8192 direcciones y 8190 hosts válidos.

8.- Cuál es el nombre del identificador de una tarjeta de red? (Nombre Completo)

MAC Media Access Control

9.- Enlistar los tipos de topología de red.

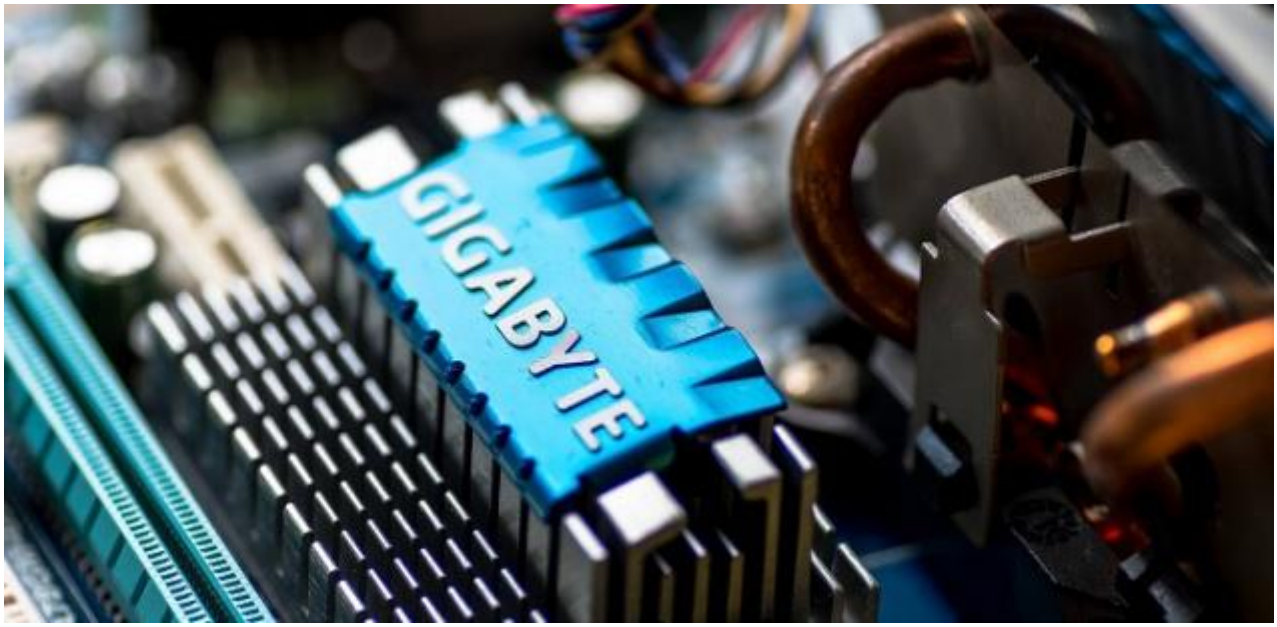
Punto a punto, bus, estrella, anillo, malla, árbol

10.- Cuáles son los rangos de ip privadas definidos por la RFC1918?

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Noticias

Fallos en los firmwares de placas Gigabyte permiten instalar virus UEFI



Expertos en seguridad han descubierto dos vulnerabilidades que afectan a algunos firmwares de placas Gigabyte, permitiendo la instalación de malware UEFI. El problema de estos fallos de seguridad es que permiten instalar virus informáticos persistentes en el equipo del usuario. Gigabyte ya está trabajando en una solución.

Ha sido la firma de seguridad Cylance la encargada de descubrir estos problemas. Han confirmado que están trabajando de la mano con Gigabyte, American Megatrends Inc. (AMI) y CERT/CC para encontrar una solución.

Desde Gigabyte también han querido aportar cierta información indicando que es cierto que existen estos problemas de seguridad. Han añadido que están buscando una solución y que es factible que en los próximos días se publique una actualización.

El problema afecta a los modelos de barebones GB-BSi7H-6500 y GB-BXi7-5775. Las versiones de firmware afectadas son las vF6 y vF2, respectivamente. Desde el fabricante han confirmado que publicarán una nueva versión para el primer modelo. Sin embargo, el segundo ya no se encuentra en producción. Esto quiere decir que el soporte ya ha finalizado, lo que provocará que los usuarios de estos equipos queden expuestos a estas vulnerabilidades.

Los fallos de los firmwares Gigabyte permiten la instalación de malware UEFI

Catalogados ya como CVE-2017-3197 y CVE-2017-3198 están cerca de ser resueltos por el fabricante. Hasta que llegue este momento aún habrá que esperar unos días. Vamos a detallar brevemente en qué consiste cada uno y las consecuencias que pueden aparecer de cara a la seguridad del usuario.

El primero de ellos afecta directamente al sistema de protección contra la escritura del firmware UEFI.

El segundo fallo está bastante relacionado con el primero. Desde el fabricante no se percataron de

la ausencia de un sistema de firmado de software. Esto permite realizar la carga de cualquier versión modificada, aunque no esté firmada. Relacionado con esta parte, encontramos también la ausencia de un simple checksum que permita comprobar la validez del archivo descargado. Teniendo en cuenta que los archivos se descargan utilizando HTTP en lugar de HTTPS, sería recomendable disponer de un sistema de verificación como este.

Estos fallos permitirían a los ciberdelincuentes ejecutar código en el modo SMM e instalar una versión maliciosa del firmware sin ningún tipo de oposición.

Analizando si hay más equipos afectados de la familia Gigabyte BRIX

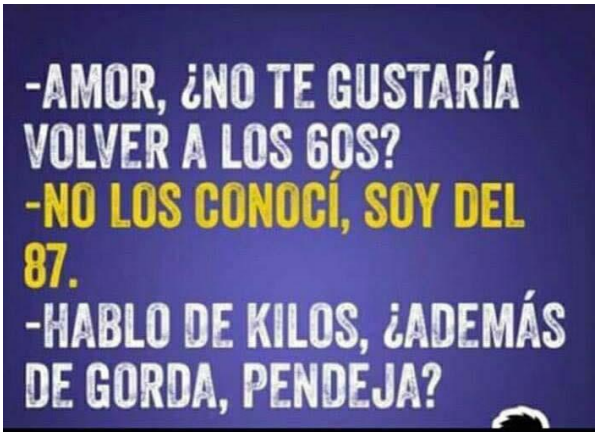
Al igual que los Intel Nuc, se trata de una familia de barebones o miniPCs. En muchos casos, son capaces de suplir las torres que se utilizan como equipos de sobremesa. Tamaño reducido y precio contenido, son dos de los atractivos de estos dispositivos. Aunque solo parece estar afectados dos modelos, desde la compañía ya han confirmado que realizarán un análisis exhaustivo para encontrar posibles problemas de seguridad.

No hay que olvidarse que un malware persistente a nivel de hardware sería un problema importante para los usuarios. En resumidas cuentas, lo que el usuario puede sufrir es una puerta trasera en su equipo que permitiría de forma remota acceder al mismo, robar información e instalar otras aplicaciones sin el consentimiento del usuario.

FUENTE:

- https://www.redeszone.net/2017/04/02/fallos-los-firmwares-placas-gigabyte-permite-instalar-virus-uefi/

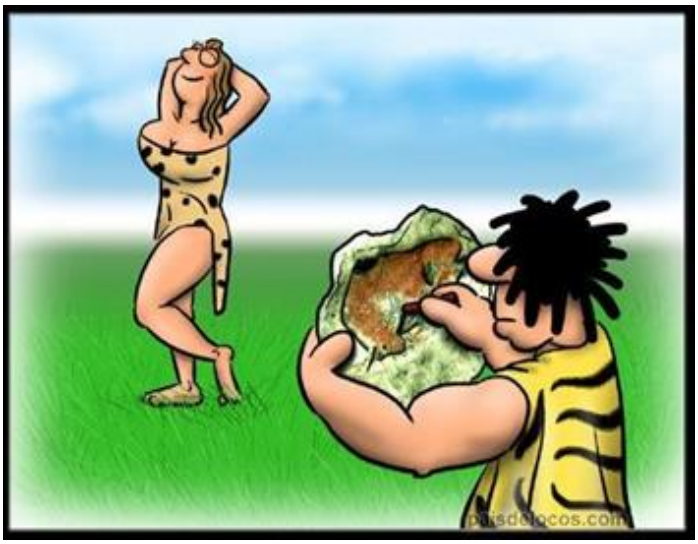
Humor


-AMOR, ¿NO TE GUSTARÍA VOLVER A LOS 60S?
-NO LOS CONOCÍ, SOY DEL 87.
-HABLO DE KILOS, ¿ADEMÁS DE GORDA, PENDEJA?


QUIERO QUE VALLAS A JUGAR AFUERA
Chattanooga Times Free Press
Bennett


Carlaaa!!!
ya llegó tu Hotmail!
WWW.ELHINODORO.COM.AR


¡LOS DINOSAURIOS EXISTEN!
LOS ENVIDIOSOS DIRÁN QUE ES UNA LAGARTIJA EN EL PARABRISAS




Primera Ley de Newton:
Un cuerpo en reposo quiere permanecer en reposo.

Robo de identidad en redes sociales, ¿qué hacer?

Internet ha revolucionado nuestra forma de comunicarnos con la gente que nos rodea y, en muchos casos, nos sirve de puente para establecer nuevos contactos profesionales o conectar con gente con aficiones o inquietudes comunes. Las redes sociales son un instrumento con el que mucha gente permanece en contacto con sus amigos, busca empleo o comparte sus fotos o vídeos, sin embargo, ante este enorme caudal de datos personales que viajan por la red, encontramos que existen personas con no muy buenas intenciones que intentarán acceder a estos datos para comerciar con ellos o, en algunos casos, suplantar nuestra identidad.

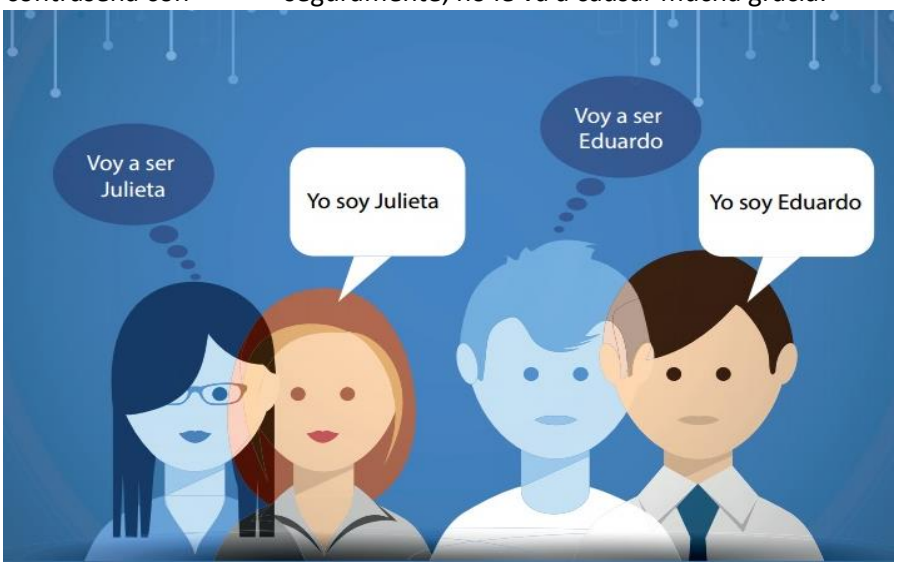
Pensemos que nuestros perfiles en Facebook y en Twitter, de alguna forma, son también nuestra tarjeta de presentación y, en unas manos inadecuadas, podrían causar un gran daño a nuestra reputación; es por ello por lo que debemos extremar las precauciones para evitar que esto suceda y, si tenemos la mala fortuna de ser víctima de una suplantación de identidad, actuar rápidamente para mitigar el daño causado y atajar el problema lo antes posible.

¿Cómo pueden robar el acceso a nuestra cuenta?

Un despiste, por ejemplo, puede propiciar un acceso no autorizado a alguna de nuestras cuentas. ¿Despistes? Sí, por ejemplo, dejar la sesión abierta en un equipo de uso compartido o dejar nuestro equipo con sesiones abiertas en el navegador y dejar que alguien lo utilice (sin nuestra supervisión), acciones a las que no les damos importancia pero que implican la exposición de nuestras cuentas a un tercero.

Al igual que avanza la tecnología, también avanzan los métodos que siguen estos "ladrones digitales" para intentar acceder a nuestros datos. FireSheep, que nos aterrorizó, no fue más que un aviso que realizó un experto en seguridad que nos mostró lo vulnerables que éramos en un congreso, en una cafetería o en un hotel en la que la red inalámbrica no estuviese cifrada.

Pero, quizás, el mayor de los riesgos esté en nosotros mismos. Una mala política personal de contraseñas puede ser un problema para la preservación de nuestra identidad digital. Usar la misma contraseña en todos los servicios web en los que estamos registrados en un gran riesgo, básicamente, porque si se compromete uno, todos lo están. Este es uno de los fallos más comunes que junto a compartir la contraseña con amigos y/o familiares, apuntar la contraseña en las notas del móvil o en un papel que guardamos en la cartera y poner una obviedad en la respuesta de las "preguntas secretas" son malas prácticas que comprometen nuestros datos. Ponérselo complicado a estos "amigos de lo ajeno 2.0" está en nuestras manos y la contraseña es algo que definimos nosotros mismos.



¿Cómo podemos darnos cuenta?

Desgraciadamente, el robo de identidad se detecta de manera reactiva, es decir, nos enteramos cuando ha sucedido y hemos notado alguno de sus efectos.

¿Efectos? Sí, imaginemos que un día intentamos acceder a nuestra cuenta de correo electrónico o a nuestro perfil en Facebook y por mucho que repetimos la contraseña, ésta aparece como invalida. Intentamos recuperar la contraseña a través de la pregunta secreta pero tampoco somos capaces de dar con la respuesta correcta; al poco, uno de nuestros amigos nos llama para preguntarnos por una publicación fuera de tono que hemos realizado en Facebook y cuando vamos al cajero automático encontramos una compra, pagada a través de PayPal, que no hemos realizado.

Aunque parezca una pesadilla o el guion de un telefilme, es algo que podría suceder y que, de hecho, sucede. Normalmente el usuario se entera después de que haya pasado y, en los casos de pishing o en los robos de documentos de identidad, las víctimas se han encontrado en listas de morosos por impagos de facturas de compras que jamás realizaron. En el mundo de las redes sociales también podría costarnos algún disgusto porque, si alguien entrase en nuestra cuenta de LinkedIn y le dejase un mensaje nada amigable a nuestro Director General, seguramente, no le va a causar mucha gracia.

¿Qué podemos hacer? ¿Cómo actuar ante una suplantación de identidad?

Si hemos sido víctima de un robo de identidad o sospechamos que algo no funciona bien debemos actuar rápidamente pero sin perder la calma.

Si aún tenemos acceso al servicio, es decir, nuestras credenciales siguen valiendo, es el momento de cambiar las contraseñas de todos los servicios a una que no guarde un patrón similar y que, además, no contenga cadenas de caracteres significativas (apellidos, nombres, ciudades, fechas de nacimiento, etc.). Dentro de lo malo, sería el escenario más favorable puesto que podríamos atajar el problema de manera

autónoma, eso sí, bueno es dar una vuelta por nuestras cuentas para revisar las publicaciones realizadas. De hecho, deberíamos de esta manera si nuestra contraseña se viese expuesta por cualquier motivo (aunque no haya indicios de robo o suplantación).

En el peor de los casos podríamos estar sin acceso a nuestra cuenta de correo y/o a cualquiera de nuestros perfiles sociales. En tal caso tenemos que mantener la calma y abordar el problema desde dos frentes: recuperar el control de nuestras cuentas y poner el caso en conocimiento de las autoridades.

Para poder recuperar el control de nuestras cuentas, prácticamente, todos los servicios tienen publicado un procedimiento que regula cómo contactar con los responsables del servicio para informar de la pérdida del control de nuestra cuenta, solicitar una suspensión temporal de la actividad de la misma o volver a recuperar el control de ésta:

- Centro de ayuda de Twitter.
- Cuentas de Facebook comprometidas y Qué hacer si tú cuenta de Facebook es vigilada por otra persona.
- Ayuda en Cuentas de Google.
- Restaurar contraseña en Hotmail.
- Cuentas en Yahoo! Comprometidas.
- Acceso fraudulento a una cuenta de Tuenti.

Además, para evitar que no nos hagan responsables de lo que hagan o publiquen desde nuestros perfiles (denuncias de terceros, inclusión en alguna lista negra, etc.), debemos informar a las autoridades de lo que ha sucedido.

¿Cómo podemos estar prevenidos?

Aunque nadie está libre de ser víctima de un robo de identidad, sí que es verdad que podemos ponérselo algo más complicado a los que intentan acceder a nuestros datos, simplemente, siguiendo unas pautas que nos ayudarán a estar mejor protegidos:

- Nunca usar la misma contraseña en todos los servicios en los que estamos registrados y, además, no usar contraseñas sencillas que sean fácilmente asociables a nosotros (fechas de nacimiento, nombres, apellidos, mascotas, etc).
- No compartir la contraseña de acceso con nadie y cambiarla tras un tiempo prudencial, mínimo tres meses al año y nunca repetir como si fuese una secuencia.
- En equipos compartidos, o de uso público, usar el modo de navegación anónimo o vaciar caché, historial, contraseñas y formularios guardados.

- Utilizar navegación segura en todos los sitios web que lo permitan, ya sea configurándolo así o usando algún complemento como HTTPS Everywhere, sobre todo, cuando accedamos a través de redes inalámbricas sin cifrar.
- Prestar atención a los sitios web a los que solemos acceder para ver si han sufrido algún cambio sustancial o, en el caso de la banca electrónica, no aparecen como sitios seguros.
- No dejar nuestro equipo sin vigilancia, desbloqueado y con sesiones abiertas.
- Jamás enviar contraseñas por correo electrónico. Servicios web como Facebook o Twitter, o la banca electrónica, nunca nos van a pedir por correo electrónico que les enviemos la contraseña y, si recibimos algún correo así, seguramente sea un intento de pishing.

FUENTES:

- https://hipertextual.com/archivo/2011/09/robos-de-identidad-que-hacer/
- http://gabrielrevelo.blogspot.com/2013_07_01_archive.html

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Abril 2017