Fiduagraria
Filial del Banco Agrario
Semilla de Inversión Sociedad Fiduciaria de Desarrollo Agropecuario S.A.

Amenazas y Riesgos en el manejo de la Información

La tendencia del mundo actual a emplear nuevos mecanismos para hacer negocios, a contar con información actualizada permanentemente que permita la toma de decisiones, ha facilitado el desarrollo de nuevas tecnologías y sistemas de información, que a su vez son vulnerables a las amenazas informáticas crecientes y por ende a nuevos riesgos.

En Fiduagraria pensando en la seguridad de nuestros clientes, usuarios y funcionarios, exponemos las principales amenazas informáticas y los posibles riesgos que podrían materializarse, para evitar que su información caiga en manos inescrupulosas o sea víctima de fraude electrónico.

SPAM

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico (SPAM) pero puede presentarse por programas de mensajería instantánea (SPIM) , por teléfono celular (SPAM SMS), por telefonía IP (SPIT) ; el objetivo de esta amenaza es recolectar direcciones de correo electrónico reales para obtener beneficios económicos, transmitir de virus, capturar de contraseñas mediante engaño (phisihing), entre otros.

Recomendaciones:

- No enviar mensajes en cadena ya que los mismos generalmente son algún tipo de engaño (hoax).
- Cuando necesite enviar un email por internet a varios destinatarios, es recomendable hacerlo con la opción con copia oculta con copia oculta con copia oculta con copia oculta (CCC), ya que esto evita que un destinatario vea, o se apodere, del email de los demás destinatarios.
- No publicar una dirección privada en sitios webs, foros, conversaciones online, etc., ya que sólo facilita la obtención de las mismas a los spammers (personas que envían spam).
- Si desea navegar o registrarse en sitios de baja confianza hágalo con cuentas de e-mails destinadas para tal fin.
- Nunca responder este tipo de mensajes ya que con esto sólo estamos confirmando nuestra dirección de e-mail y sólo lograremos recibir más correo basura.
- Es bueno tener más de una cuenta de correo (al menos 2 o 3): una cuenta laboral que sólo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

HOAX

Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena; algunos informan sobre virus desastrosos, otros apelan a la solidaridad con un niño enfermo o cualquier otra noble causa, otros contienen fórmulas para hacerse millonario o crean cadenas de la suerte como las que

existen por correo postal. Los objetivos que persigue quien inicia un hoax son: alimentar su ego, captar direcciones de correo y saturar la red o los servidores de correo.

Recomendaciones

- No exponga en sitios públicos su dirección electrónica ni la de sus contactos
- Haga caso omiso a este tipo de mensajes y elimínelos inmediatamente de su buzón. No los reenvíe.

Código malicioso (malware)

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario; el término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

El término malware incluye:

- Virus: Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y 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.
- Gusanos: Tiene la propiedad de duplicarse a sí mismo; los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.
- Troyanos: Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al ejecutarlo ocasiona daños; los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés backdoor) que permite la administración remota del computador a un usuario no autorizado.
- Rootkits: Es un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

- Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
- Keyloggers: Son programas maliciosos que monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador; por ejemplo, al introducir un número de tarjeta de crédito el keylogger guarda el número, posteriormente lo envía al autor del programa y este puede hacer pagos fraudulentos con esa tarjeta.
- Stealers: También roban información privada pero sólo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador.
- Adware: Es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalar el programa o mientras se está utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés.
- Crimeware: Ha sido diseñado, mediante técnicas de ingeniería social u otras técnicas genéricas de fraude en línea, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas en línea de compañías de servicios financieros o compañías de venta por correo, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.
- Pharming: Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.
- Ransomware: Es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Normalmente se transmite tanto como un troyano como un gusano, infectando el sistema operativo, con un archivo descargado o explotando una vulnerabilidad de software.

Recomendaciones

- Instalar oportunamente las actualizaciones (parches) de seguridad del sistema operativo de su PC.
- Tener instalado y actualizado un sistema de antivirus y antispyware.

- No abras los archivos adjuntos del correo electrónico que no han sido solicitados o procedente de personas desconocidas.
- Usa en internet un navegador actualizado.
- Solo descarga aplicaciones desde sitios seguros y ante cualquier duda chequea la dirección del archivo.
- Evitar navegar por páginas no seguras o con contenido no verificado.
- Impide que personas que no tienen conocimiento o son imprudentes usen tu equipo. Activa las extensiones de archivos para poder identificar los archivos que de forma engañosa terminan con la extensión EXE.

Ingeniería Social

Es una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema de información; es el arte de conseguir lo que nos interese de un tercero por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos. Las acciones realizadas suelen aprovecharse de engaños, tretas y artimañas para lograr que un usuario autorizado revele información que, de alguna forma, compromete al sistema.

Los fines generales de la ingeniería social son:

El usuario es tentado a realizar una acción necesaria para dañar el sistema: este es el caso en donde el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto o abrir la página web recomendada que terminará dañando el sistema. • El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del phishing, en donde el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza.

Recomendaciones:

- Evite brindar información que pueda comprometer la seguridad personal o de los sistemas de información; datos como usuario, contraseña, fecha de nacimiento, nombres de familiares, empresas, números de tarjetas, situación social, salud, costumbres, datos económicos, etc. pueden ser utilizados por una persona inescrupulosa para efectuar acciones dañinas.

Phishing

Es una modalidad de estafa con el objetivo de intentar obtener de un usuario información personal como: contraseñas, cuentas bancarias, números de tarjeta de crédito, número de identificación, direcciones, números telefónicos, entre otros, para luego ser usados de forma fraudulenta; para esto el estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas, de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

Recomendaciones:

- Fiduagraria NUNCA le solicitará información personal o financiera a través de correo electrónico, llamada telefónica o mensaje corto (SMS).
- Recuerde que para registrarse en nuestro portal web o actualizar su información, siempre debe ingresar digitando la dirección www.fiduagraria.gov.co
- Ante la recepción de correos electrónicos sospechosos con temas relacionados con Fiduagraria, comuníquese a nuestra línea de atención al cliente a nivel nacional 01 8000 95 9000 o en Bogotá al 5802080.

Vishing

El atacante cuando se vale de la técnica de vishing, envía mensajes de correo fraudulentos que sugieren llamar a un número de teléfono, en el cual un contestador automático va solicitando toda la información requerida para acceder a nuestros productos a través de medios electrónicos.

Un ejemplo de vishing es:

1. El criminal configura un war dialing (hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún otro ordenador) para llamar a números telefónicos en una determinada región.
2. Cuando la llamada es contestada, una grabación toca y alerta que al "consumidor" que por ejemplo su tarjeta de crédito está siendo utilizada de forma fraudulenta y que este debe llamar

al número que sigue inmediatamente. El número puede ser un número gratuito falseado para la compañía financiera que se pretende representar.

3. Cuando la víctima llama a este número, es contestada por una voz computarizada que le indica al "cliente" que su cuenta necesita ser verificada y le requiere que ingrese los 16 dígitos de su tarjeta de crédito.
4. Cuando la persona provee la información de su tarjeta de crédito, el visher (atacante) tiene toda la información necesaria para realizar cargos fraudulentos a la tarjeta de la víctima.
5. La llamada puede ser también utilizada para obtener detalles adicionales como el PIN de seguridad, la fecha de expiración, el número de cuenta u otra información importante.

Recomendaciones

- Cuando reciba llamadas de números desconocidos valide con quien se está comunicando y no suministre información confidencial si no está seguro de quién la está solicitando y el motivo.
- Recuerde que para hacer transacciones usted es quien inicia la comunicación con las líneas telefónicas que Fiduagraria ha definido.

Smishing

Es un tipo de delito informático o actividad criminal usando técnicas de ingeniería social empleado mensajes de texto dirigidos a los usuarios de telefonía celular.

El sistema emisor de estos mensajes de texto o incluso un individuo el cual suele ser un spammer, intentará suplantar la identidad de alguna persona conocida entre nuestros contactos o incluso una empresa de confianza, solicitando el ingreso a una dirección en internet o un número de Call center falsos, con el fin de tratar de robar dinero o adquirir información personal.

Recomendación

- Generalmente los mensajes de texto SMS recibidos anunciando premios, bonos, descuentos son falsos y sólo buscan robar su dinero o información personal con fines criminales, evite comunicarse con los teléfonos o sitios web que le indican, reporte este tipo de mensajes en caso de que se relacionen con Fiduagraria y elimine los mensajes de su equipo móvil.