Ministerio de Justicia y Derechos Humanos

Dirección Nacional de Protección de Datos Personales

Recomendaciones de la Dirección Nacional de Protección de Datos Personales

Internet es una herramienta de mucha utilidad y el uso descuidado, como por ejemplo el acceso a páginas de dudosa procedencia, puede provocar daños en su pc y a su privacidad. Esto se realiza por medio de programas maliciosos que se introducen al sistema. Estos programas se dedican al robo de datos personales y a cuentas de credito, mientras que otros son utilizados con fines publicitarios. Estos ingresan por diferentes medios y los antivirus tradicionales no suelen detectarlos. Para eliminarlos se requieren programas especiales

La Dirección Nacional de Protección de Datos personales ofrece la siguiente información sobre los peligros de la web y las recomendaciones para que usted pueda navegar mas seguro por internet, con el objeto de contribuir a la protección de su privacidad y sus datos personales.

Peligros en la web y en el correo electronico:

- El **software malicioso** son programas también conocidos como **malware.** Puede ser un virus que parece inocente, con alguna imagen en la pantalla que aparece y desaparece, hasta un virus que destruya toda la información. Este software es muy peligroso para las empresas, porque algunos programas fueron creados con propósitos criminales, tales como las transferencias de dinero, espionaje industrial, etc..
- El **software espía** o **spyware** registra todo lo que el usuario hace con el propósito de conocer sus preferencias para enviarle publicidad relacionada con su perfil.
- El **spam** consiste en todo lo que el usuario recibe en su casilla de correo electronico, sin haberlo solicitado. Hay diferentes tipos de spam que pueden llegar a nuestra Bandeja de Entrada. Entre estos se destacan los mas perjudiciales como el Hoaxes, los Fraudes y los Scams.

  a) **Hoaxes o *bromas de mal gusto***: Un mail que invita a hacer algo que resulta perjudicial. Hace creer al usuario que debe hacerlo para evitarse problemas. Una broma que circuló hace un tiempo invitaba a buscar en la máquina un archivo determinado, diciendo que si estaba implicaba que la máquina se encontraba infectada y que la única forma para solucionarlo era borrarlo inmediatamente. Se trataba en realidad de un archivo esencial del sistema operativo, por lo que nuestra máquina dejaba de arrancar a partir de entonces (por ejemplo, archivos tales como jdbmgr.exe, sulfbnk.exe, esenciales para el sistema operativo).

  b) **Frauds o fraudes**: Un mail que implica un comportamiento deshonesto, cuyo objetivo es hacer dinero, donde alguien se hace pasar por quien no es, o nos hace creer algo que no es cierto, sugiriendo que sigamos un procedimiento por el cual seremos perjudicados económicamente.

  c) **Scams:** Los Scams son una forma de Fraude. Se trata de un mail que atrae el interés del usuario y que esconde una maniobra deshonesta. En algunos casos ofrece ganar dinero fácilmente, para lo cual hace una propuesta que,

al seguirla, pondrá en grave riesgo el patrimonio del usuario e incluso su buen nombre y honor. A modo de ejemplo, podemos citar un mail que da la noticia de que se ha ganado un importante premio de lotería o que un señor africano (Nigerian Scam) tiene que cobrar mucho dinero y tiene un impedimento para hacerlo en su país y necesita que el usuario se lo cobre.

d) **Phishing**: Se recibe un mail proveniente, en apariencia, de una entidad de reconocida trayectoria y que invita a visitar el Web Site de la empresa para actualizar datos. El vinculo en realidad lo remite a una página falsa con la intención de robar datos personales, que puede incluir incluso número de cuenta bancaria y palabra clave. Aún cuando en esa página no complete ningún dato el sólo hecho de haber ingresado lo expone a un ataque. Existe una organización que lucha contra el Phishing, Scam y otros fraudes, cuya dirección es: www.antiphishing.org. Para evitar este tipo de engaño siempre es necesario ver el dominio (identidad) de la pagina web que se visita. Como por ejemplo estar atento a la extensión, si es un dominio www.jus.com.ar, definitivamente daremos cuenta que es falso.

e) **Pharming**: Es más difícil de detectar, ya que a diferencia del Phishing, la persona que sufre el Pharming visita un Web Site malicioso en forma totalmente inadvertida. Se debe a que el proveedor del servicio de Internet sufrió un ataque en su DNS, el cual quedó "envenenado" (DNS, Domain Name Server, es el lugar donde se traduce la dirección que nosotros escribimos –alfanumérica y fácil de recordar- en la verdadera dirección –numérica y difícil de recordar pero entendida por la máquina-). A raíz de que el DNS quedó envenenado, ponemos correctamente el lugar que queremos visitar, pero el DNS nos manda a un lugar incorrecto: un Web site malicioso donde sufriremos un ataque a nuestra privacidad. Es responsabilidad del "Service Provider" de Internet proteger el DNS para que esto no ocurra.

Recomendaciones

1) **Mantenga actualizado el software**. Es muy importante contar con un buen antivirus y un antispyware. También actualice cada 15 días su antivirus y su Sistema Operativo.
2) **Utilice exploradores que no tengan muchas fallas de seguridad**.
3) **Sea cuidadoso con los lugares que visita** y mucho más cuando esos lugares le hacen instalar programas especiales, por ejemplo "dialers" (marcadores telefónicos que, en algunos casos, pueden marcar números internacionales automáticamente) ofreciendo disfrutar del lugar con fotografías, música y videos. Como resultado de su visita puede tener instalado un espía en su máquina que va a informar al dueño de la página todo lo que usted hace minuto a minuto.
4) **Sea cuidadoso con los correos que abre. No basta conocer el emisor para abrir el correo con confianza**, ya que no existe ningún mecanismo para autenticar el nombre del remitente. La persona que envía puede colocar en el campo "De" o "From" el nombre o la frase que desee, y este nombre es el que se muestra en el mensaje al recibirse. **Cualquier correo, cualquiera sea el asunto que un mensaje tenga, puede ser contaminante** (es sencillo para un programador emitir mensajes con el mismo contenido malicioso y cientos de asuntos distintos). **Si la redacción del mail no concuerda con lo que habitualmente suele recibir del remitente, no lo abra**. Verifique por e-mail o teléfono si realmente esa persona amiga/conocida le mandó ese mail y, sólo una vez verificado que no existen problemas, proceda a abrirlo. O en caso contrario elimínelo rápidamente para evitar cualquier contratiempo.

5) Salvo circunstancias muy especiales **no se haga partícipe de cadenas de mails**, ni crea en frases que le incentivan a participar en las mismas diciendo algo así como: "*Atención: no es una broma, funciona. Entonces, date gusto, regálate …*", etc.
6) **Utilice la opción "copia oculta" para enviar mails.** Le evitará problemas a los destinatarios ya que el mail, en camino a su destinatario pasa por equipos intermedios que tienen acceso al contenido del mensaje, y pueden utilizarse para recopilar direcciones para después utilizarlas para enviar correo SPAM.
7) Si usted tiene contratada banda ancha, la cual no paga por tiempo de conexión, **no la deje "conectada" en forma permanente las 24 horas del día,** ya que el tiempo prolongado de conexión aumenta la probabilidad de éxito de un eventual atacante que encuentre su máquina al barrer, al azar, direcciones de Internet. Si el atacante tiene éxito, debido a vulnerabilidades no protegidas del sistema, puede instalar en la máquina programas maliciosos o incluso utilizarla como iniciante de otros ataques dirigidos a terceras máquinas.
8) **Solamente llene formularios en la WEB en los que se esté utilizando el protocolo https://** (*utiliza un Servidor Seguro con encriptación –ilegible para alguien que lo "atrapa" en el medio e intenta leer- de datos entre el Servidor y su máquina*), en lugares que le merezcan confianza, y solamente en los casos en los que el llenarlo le proporcione un real beneficio (por ejemplo, acceso a información que usted necesita consultar).
9) **Recomiende a sus hijos que no den ninguna clase de dato respecto a su propia persona ni de ningún familiar directo** y que el uso que le den al Chat sea el mismo tanto en presencia de los padres como en ausencia de los mismos. Considere seriamente, también, la ubicación de la PC en un área "pública" de la casa (un lugar donde la pantalla esté siempre a la vista de los padres). Instale programas para evitar que sus hijos accedan a páginas prohibidas.
10) **No confíe** ciegamente **en lo** que está **publicado en INTERNET**. **Cualquiera puede publicar lo que quiera y no existe un órgano fiscalizador** que controla que lo que está publicado en la WEB no sea malicioso ni que sea verdadero. Procure seleccionar lo que consulta tratando de quedarse con aquello que sea realmente confiable. Sea crítico al analizar el contenido, y deseche páginas o "sites" completos donde observe errores, inexactitudes, superficialidad u otro atributo que le hagan perder confianza en lo allí publicado.
11) **NIC (Network Information Center),** es el organismo que administra y registra los dominios en argentina y el mundo. Usted puede visitar www.nic.ar y ver quienes son los responsables de los sitios que usted visita, en Argentina.

Ponemos a su disposición la información de contacto de esta Dirección Nacional para que pueda evacuar todas sus dudas y obtener el asesoramiento en el ejercicio de los derechos que le acuerda la Ley de Protección de Datos Personales.

También le facilitamos la información para que pueda contactarse con la División Delitos Informáticos de la Policía Federal Argentina para asesorarse ante la posible comisión de delitos vinculados con el uso de la informática.