Protección de datos y equipos

Por Educ.ar

En sus comienzos, internet se utilizaba básicamente para buscar información y emitir/recibir mensajes por e-mail. Luego comenzó a popularizarse el uso de los blogs personales, la posibilidad de pagar las cuentas por medio de internet o de subir fotos e información personal en las redes sociales.

Estos datos cargados/publicados quedan circulando en un mundo virtual y la posibilidad de que sean utilizados por malas aplicaciones está siempre latente.

Existen muchas herramientas que ayudan a evitar este tipo de inconvenientes, como antivirus, *firewalls*, filtros y contraseñas. En internet, como en el resto de la vida cotidiana, existen riesgos y diversas maneras de prevenirnos y actuar con responsabilidad frente a las amenazas. Para saber de qué se trata y actuar en consecuencia, les acercamos información sobre estos y otros fenómenos existentes en la web.

Los datos personales

El nombre y apellido; el número del DNI.; las huellas dactilares, una fotografía, información sobre la salud, las creencias, los gustos, entre otros, constituyen la base de nuestros datos personales. Aquí les contamos sobre los derechos de los usuarios al respecto y por qué un tercero no puede utilizarlos arbitrariamente.

Los datos personales **permiten identificarnos como individuos únicos y singulares**; son usados en situaciones específicas y tienen que ser solicitados con alguna justificación.

Habitualmente en internet los chicos quieren completar algunos formularios por distintas razones: para abrir una cuenta de e-mail, jugar un juego o adquirir algún producto. Los sitios deben hacerse responsables de que estos datos no se filtren con otros fines.

Los chicos y chicas tienen que ser conscientes de que ellos son dueños de sus datos personales y que no están obligados a facilitarlos. **Ningún tercero puede**

exigir los datos personales a un menor, y en caso de requerirlo debe justificar el motivo.

Los chicos y chicas **nunca deben completar estos formularios solos**, siempre debe haber un adulto que controle qué tipos de datos se solicitan y verificar qué utilización tendrán los mismos.

La idea de los datos privados

Aunque internet existe hace ya muchos años, aún no hay marcos regulatorios muy claros que delimiten los derechos y obligaciones de los usuarios que publican o manipulan información en la red. Si bien en algunos países los aspectos legales están más desarrollados, en otros es una cuenta pendiente a la espera de una discusión.

Actualmente en la Argentina, como en el resto del mundo, existen normas que regulan el tratamiento de la información y de los datos personales; como la Ley de Protección de Datos Personales (Ley 25.326), la Ley de Delitos Informáticos (Ley 26.388), y la Ley de Derecho de Autor (Ley 11.723), entre otras.

La Ley 25.326, por ejemplo, establece que los datos personales no pueden procesarse sin el consentimiento expreso del titular, salvo contadas excepciones. Todo aquel que adquiera, procese o ceda datos personales sin el consentimiento del titular estará realizando una actividad ilícita.

Quizás comentarles esto a los chicos suene complicado y aburrido. Pero aun sin entrar en el detalle de las leyes, es conveniente explicarles que deben preservar algunos datos y que no pueden brindar información de índole privada a cualquier persona o institución.

En caso de que se presente una situación en la que se requieren datos personales, deben saber que es bueno contar con la supervisión de un adulto para brindar cualquiera de esos datos.

Mensajes engañosos

La palabra *phishing* (del inglés *fish*: pescar) consiste en una forma de engaño mediante la cual se envía un mensaje que funciona como un anzuelo a una o varias personas, intentando convencerlas para que revelen sus datos personales. Luego, la información recolectada suele utilizarse para diversas acciones fraudulentas o delictivas.

Es frecuente que lleguen a la cuenta de correo electrónico e-mails de desconocidos que solicitan ciertos datos para ganarse un premio. El modo de difusión más utilizado para realizar un ataque de *phishing* suele ser el correo electrónico. Estos correos suelen ser muy convincentes y simulan haber sido enviados por una entidad conocida y confiable. En los mensajes suelen alegarse motivos creíbles y a continuación se solicita ingresar a un sitio web para modificar o verificar una serie de datos personales.

Los chicos y chicas —e incluso los adultos— que navegan en internet pueden caer ante los mensajes-anzuelo y ser «pescados». Confiados, suelen cargar sus datos, corriendo el riesgo de que sean usados en algún momento por un tercero con malas intenciones.

Es responsabilidad de los padres advertir a sus hijos sobre este tipo de correo para que eviten publicar datos personales. Dependiendo de su edad, el joven podrá comprender la seriedad del problema y darse cuenta de **cuándo no es conveniente subir ciertos datos a la red**.

Más sobre el *phishing*

Detrás de estos enlaces que parecen prometer entretenimiento o premios hay un sitio falsificado (aunque a veces sean similares, o incluso idénticos, a los de páginas web confiables). Asimismo, estos sitios tienen direcciones web que pueden confundir al usuario desprevenido por su parecido con las direcciones web de cualidades prestigiosas En la mayoría de los casos, el texto del enlace escrito en el correo electrónico es la dirección real del sitio web. Sin embargo, si el usuario hace clic sobre ese enlace, se lo redirige a otra página falsa.

También existen casos donde el usuario recibe un mensaje SMS en su teléfono celular, o una llamada telefónica, en la que mediante técnicas similares se intenta convencerlo para que llame a un número de teléfono indicado en el mensaje. Al llamar a ese número, un sistema automatizado —haciéndose pasar por un organismo verdadero— suele solicitarle sus datos personales, que luego serán utilizados sin su autorización.

Algunas medidas preventivas contra el *phishing*

- Si reciben un correo electrónico solicitando información personal, no respondan. Si el mensaje los invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo hagan. Las organizaciones que

trabajan seriamente están al tanto de este tipo de actividades y por lo tanto no solicitan información sensible por correo electrónico. Tampoco te contactan por teléfono, ni mediante mensajes SMS o por fax.

- No envíen información personal usando mensajes de correo electrónico. El correo electrónico, si no se utilizan técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial.

- Evitar ingresar a sitios web de entidades financieras, comercio electrónico, o a brindar datos personales desde un cíber, locutorio u otros lugares públicos. Las computadoras instaladas en estos lugares podrían contener *hardware* o programas maliciosos destinados a capturar sus datos personales.

- Verificar los indicadores de seguridad del sitio web donde vas a ingresar información personal. Si es indispensable realizar un trámite o proveer información personal a una organización por medio de su sitio web, escribir la dirección web por tu cuenta en el navegador y buscar los indicadores de seguridad del sitio.

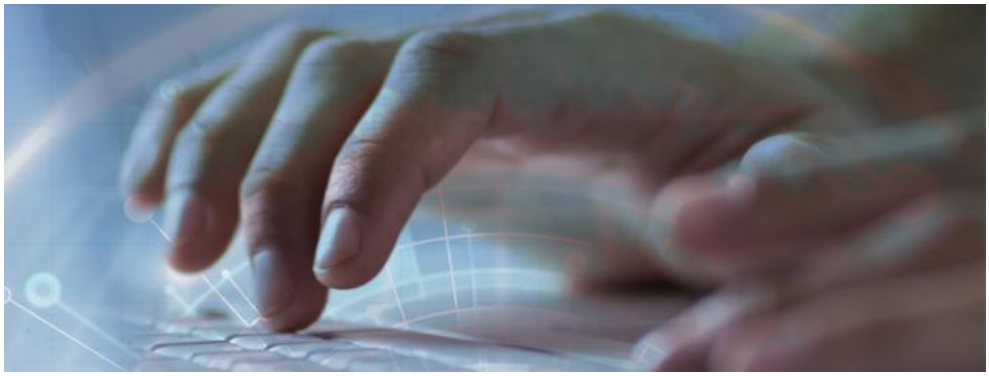
- Al acceder al sitio web, deberán notar que la dirección web comienza con https://, donde la letra «s» indica que la transmisión de información es segura. Verificar también que en la parte inferior de sus navegadores aparezca la imagen de un candado cerrado.

- Hay que mantener actualizado el *software* de la computadora. Instalar las actualizaciones de seguridad del sistema operativo y de todas las aplicaciones que utilicen, especialmente el programa antivirus. La mayoría de los sistemas actuales permiten configurar estas actualizaciones en forma automática.

- No descarguen ni abran archivos de fuentes no confiables. Estos archivos pueden tener programas maliciosos que podrían permitir a un tercero acceder a sus computadoras y, por lo tanto, a toda la información que tengan almacenada.

En los últimos tiempos, y junto con la profusión de las redes sociales, los blogs y los dispositivos de chateo, mucha información que antes circulaba en pequeños círculos íntimos cobró nuevas dimensiones. Consciente o inconscientemente, muchos adultos, jóvenes y niños hacen públicos todo tipo de datos personales, que pueden ser objeto de captura y reutilizados con diversos fines.

Hay que generar conciencia de que **no todo lo que se publica se puede luego borrar fácilmente**. Es importante comenzar a manejar criterios sobre el tipo de información que merece ser compartida con otros usuarios y cuál no. Adultos y adolescentes en familia, y en la escuela, deben conversar sobre el tema de la seguridad informática y consensuar pautas para el uso responsable de las TIC.



Amenazas en la web

Las palabras virus, antivirus y troyanos se oyen con frecuencia. Lo mismo sucede con programas maliciosos, el *spam* y los engaños fraudulentos. Todo suena amenazante y peligroso. Pero existen formas de enfrentarse a este tipo de situaciones sin dejar de utilizar los beneficios de la web.

Los programas maliciosos

Un **código o programa malicioso** (*malware*) consiste en un programa de computadora escrito para producir inconvenientes, destrucción y/o quebrantar la seguridad de un equipo o sistema informático.

Se diferencian en:

- **Virus**: para activarse en la computadora, suelen requerir de alguna interacción por parte del usuario (por ejemplo, abrir un archivo adjunto que recibimos por correo electrónico). Hoy también existen virus que afectan los teléfonos celulares.

- **Caballos de Troya o troyanos**: son programas que tienen una funcionalidad conocida (por ejemplo, un juego) pero además tienen una función oculta (como capturar las claves que escribe el usuario y mandarlas en un mensaje de correo electrónico a otra persona).

- Gusanos: se reproducen sin necesidad de interacción de los usuarios, por ejemplo atacando servicios de red vulnerables.

Estas tres variantes suelen ser las que más atacan a las máquinas, y en general los chicos están al tanto. Pero a veces la tentación de abrir un archivo o bajar algo de internet produce la activación de este tipo de programas maliciosos, que requieren la intervención de un técnico para arreglar el daño que hayan provocado.

Algunas consecuencias que pueden generar los programas maliciosos:

- Borrar archivos del disco rígido para que la computadora se vuelva inoperable.
- Infectar una computadora y usarla para atacar a otras.
- Obtener información sobre el usuario, los sitios web que visita y sus hábitos en la computadora.
- Capturar las conversaciones activando el micrófono o viendo al usuario, con la activación de la Webcam.
- Ejecutar comandos en la computadora como si lo hubiera hecho el usuario.
- Robar archivos del equipo, por ejemplo aquellos con información personal, números de serie (licencia) de programas instalados, etcétera.

El *spam*: los correos interminables

Es muy frecuente recibir en la casilla de correo mensajes de gente desconocida, que brindan información que no solicitamos. Estos mensajes no solicitados (más conocidos como *spam*) suelen incluir publicidad, y muchas veces contienen información falsa o engañosa. Algunas de las técnicas que utilizan los *spammers* (aquellos que envían mensajes no solicitados para rédito propio o para terceros), para obtener direcciones válidas de correo electrónico, incluyen:

- Búsqueda de direcciones en páginas web y foros.
- Captura de direcciones en cadenas de correo.
- Compra de bases de datos de direcciones de correo.
- Acceso no autorizado en servidores de correo.

Por tanto, es conveniente tener en cuenta algunas reglas de comportamiento con respecto a estos envíos de mensajes no solicitados:

- No dejar la dirección de correo electrónico en cualquier formulario o foro de internet en el que no nos interese participar.
- No responder a los correos no solicitados.
- No enviar respuesta a la dirección que figura, para evitar envíos posteriores.
- Configurar filtros o reglas de mensaje en el programa de correo para filtrar mensajes de determinadas direcciones.
- No configurar respuesta automática para los pedidos de acuse de recibo.
- No responder a los pedidos de acuse de recibo de orígenes dudosos.

Las cadenas de e-mails: el eterno pedido de ayuda

Una de las técnicas más conocidas para fomentar los reenvíos de mensajes, obtener direcciones de correo y armar bases de datos con ellas es la conocida **cadena de correos electrónicos**. En estas cadenas se apela a la solidaridad del receptor solicitando el reenvío con fines benéficos; o se advierte sobre ciertas cuestiones, pidiendo que se retransmita el alerta.

Aunque es conocido que esas cadenas son falsas y tienen intenciones muy distintas de ayudar, por ejemplo, a alguien a operarse, siempre se genera un nuevo tema y en el **Asunto** del cuerpo del correo suele aparecer la leyenda: «Esto es verdad, por favor léelo». Y adultos y adolescentes suelen caer en la trampa.

Seguro se preguntarán quién hace esto y para qué. Las direcciones de correo electrónico incluidas en los mensajes suelen ser utilizadas para integrar bases de datos, que luego son empleadas para enviar *spam*. También pueden ser capturadas por virus informáticos, como fuente de direcciones válidas a las cuales reenviarse.

Es conveniente no reenviar compulsivamente estos mensajes. Este comportamiento suele extenderse porque es común pensar que reenviar un mensaje no tiene costo alguno (en comparación con una llamada telefónica o un envío postal). Sin embargo, debemos pensar que estamos comprometiendo datos de terceros, tiempo propio y de otros destinatarios.

¿Cómo navegar seguros en la web?

Consejos para navegar seguros en la web

Sin ánimo de generar temor, ni crear una idea negativa sobre el uso de internet y las nuevas tecnologías de la comunicación y la información, aquí van algunos consejos básicos para que los adultos, los chicos y las chicas puedan **disfrutar de la red minimizando riesgos**.

Lo importante es estar atentos a ciertas cuestiones para evitar ser engañados.

A veces un *link* (enlace) puede ser engañoso y llevar a un sitio diferente del que figura en el texto del enlace. Para evitar caer en esta trampa, se recomienda, ante la primera impresión de desconfianza:

1. Verificar el destino de los enlaces con la opción **Propiedades** (utilizando el botón derecho del *mouse*) para corroborar que sea el mismo que se menciona en el texto del enlace.
2. Evitar acceder a sitios desconocidos o poco confiables, ya que los mismos pueden incluir contenidos que permitan descargar y ejecutar programas maliciosos en nuestra computadora.
3. Asegurarse de que el navegador no acepte la instalación de *software* descargado de internet en forma automática.
4. Si se necesita introducir información sensible en un sitio web, asegurarse de que la página es segura (notar que la dirección web comience con **https://**).
5. Establecer normas para el uso adecuado de las contraseñas, de forma de prevenir que sean vulneradas y utilizadas por intrusos para acceder a los sistemas de forma no autorizada.

Para ello:

- Cuidar de no ser observados al escribir nuestra clave.
- No observar a otros mientras lo hacen.
- No escribir la clave en papeles, ni en archivos sin cifrar.
- No compartir claves con otros.
- No pedir las claves de otros.
- No habilitar la opción de recordar claves en los programas que utilicen en equipos compartidos.
- No enviar claves por correo electrónico.
- No mantener una contraseña indefinidamente (se recomienda cambiarla con cierta regularidad).
- No abrir archivos adjuntos de origen desconocido.
- No abrir archivos adjuntos que no esperan recibir, aunque les parezca que su origen es conocido.

Dispositivos de protección

Aquí les brindamos algunos dispositivos y recursos para proteger la computadora de las principales amenazas externas, sin olvidar que **la mejor defensa es la precaución y el conocimiento**.

***Firewall*, filtros y antivirus**

El ***firewall*** consiste en un sistema diseñado para evitar accesos no autorizados desde o hacia un equipo. Todos los mensajes, códigos o programas que ingresan a la computadora son filtrados por este sistema y pasan a través suyo, al tiempo que son examinados y bloqueados aquellos que no cumplan con determinados criterios de seguridad.

Los **filtros** son programas o configuraciones que permiten restringir el acceso a sitios o contenidos considerados inconvenientes para los más chicos. Estos dispositivos pueden seleccionar contenidos, establecer horarios de uso y ofrecer

registros de los sitios visitados.

De esta manera no hace falta que los padres, tutores o familiares estén presentes para controlar qué sitios visitan los chicos. Directamente se determinan el tipo de páginas que se pueden ver y se sabe que, al menos en el hogar, no se van a enfrentar con cierto tipo de contenidos.

Si bien pueden llegar a bloquear páginas que no son adecuadas, muchas veces también impiden la lectura de otros sitios o páginas que son correctas y que tienen información necesaria para los chicos. Otros funcionan a partir de listas que se realizan en los servidores filtro, que son los que deciden qué contenidos son convenientes y cuáles no.

Nuevamente, **no son la opción más recomendable ni pueden reemplazar a la educación sobre uso de la web ni al acompañamiento**.

Para disminuir las amenazas que presentan los códigos o programas maliciosos, se suele utilizar programas **antivirus**. Sin embargo, es importante resaltar que estos programas no son siempre efectivos, ya que suelen detectar el código malicioso en base a patrones conocidos; es decir que no detectan automáticamente los últimos desarrollos. Por eso es conveniente mantener el antivirus actualizado, aunque no puedan dar garantías totales.

Para averiguar más sobre el tema lean el artículo «Seguridad y uso responsable de las TIC» de **educ.ar**.

En el artículo «Las dos caras de la moneda», podrán analizar cuál es la mejor manera de acompañar a los chicos cuando utilizan internet.