

Privacidad y nuevas tecnologías

El poder en las manos del usuario

Autor: Sebastián Bortnik



El presente trabajo es publicado bajo una licencia de Creative Commons, Atribución-No Comercial-Compartir Obras Derivadas Igual 2.5 Argentina

Usted es libre de:

- copiar, distribuir, exhibir, y ejecutar la obra.
- hacer obras derivadas de ella.

Bajo las siguientes condiciones:

- Usted debe atribuir la obra en la forma especificada por el autor o el licenciente.
- Usted no puede usar esta obra con fines comerciales.
- Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.



<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>

Resumen

La tecnología es hoy parte de la cotidianidad de los ciudadanos. Cualquier individuo económicamente incluido en su sociedad utiliza la tecnología diariamente. Como consecuencia, depositamos cada vez más información personal en tecnologías de terceros de las cuáles no siempre podemos conocer los niveles de confidencialidad que manejan.

La privacidad del usuario se ve afectada por la implementación de las nuevas tecnologías en la vida cotidiana del usuario. Los peligros de finalizar como una sociedad sin privacidad, parecen no ser tan lejanos.

El paper que se desarrolla a continuación, es una extensa reflexión personal del autor acerca de cómo las nuevas tecnologías, la privacidad, y la seguridad, están ligadas de una u otra forma, cuáles son los roles que cumplen o pueden cumplir los diferentes actores que se presentan; y si todavía estamos a tiempo de vivir en un mundo donde la privacidad del individuo, siga siendo un valor respetado y valorado.

Las últimas dos secciones representan las diferentes acciones que, según el autor, el usuario puede tomar para comprender y vivir su relación con las tecnologías y las consecuencias de cada una de ellas.

- "*¿Existe el Gran Hermano?*" - Winston
- "*Claro que existe. El Partido existe. El Gran Hermano es la encarnación del partido.*" - O'Brien
- "*¿Existe en el mismo sentido en que yo existo?*" - Winston
- "*Tú no existes.*" - O'Brien

1984 George Orwell

"Esa manía de hacer las cosas en privado, lo que en la práctica se traduce en no hacer nada."

Un Mundo Feliz Aldous Huxley

Índice

Introducción	6
Seguridad y Privacidad	7
Web 2.0 y nuevas tecnologías en el siglo XXI	8
Jaque a la identidad	13
¿Quién es el responsable?	15
Dos opciones: inclusión o privacidad	18
Conclusión	19
Glosario	21
Bibliografía	22

Nota: Todas las citas presentadas en el comienzo de cada sección, pertenecen al libro '1984' de George Orwell.

Introducción

Hay quienes dicen que no hay mejor manera de definir algo que a través de lo que no es.

El presente no es un trabajo de investigación técnica ni profunda sobre seguridad; no es un relevamiento exhaustivo de la situación a través de sus actores ni es un documento cuyas conclusiones, presenten hechos fácticos y concretos, aptos para ser referencia en la materia.

Por el contrario, el presente trabajo es una extensa reflexión, basada especialmente en mi trabajo diario relevando las noticias más importantes en materia de seguridad informática a nivel mundial. Esto, sumado a los conocimientos y experiencias que generan mis trabajos en tecnología y la interacción con otros actores en la vida cotidiana como familiares o amigos, son las fuentes de conocimiento para la realización del presente.

La tecnología hoy ya no es más una opción. Cualquier individuo económicamente incluido en su sociedad, incluso en países del tercer mundo como desde el que escribo, utiliza la tecnología diariamente. Sin embargo, depositamos cada vez más información personal en tecnologías de terceros de las cuáles no siempre podemos conocer los niveles de confidencialidad que manejan. Sumado a esto, nuevos paradigmas de privacidad surgen en la población.

La información personal, ya no es más un simple dato que solo puede ser transmitido de boca en boca, sino que muchas veces son datos accesibles por cualquier individuo del planeta.

El dilema, en segunda instancia, lo representan los daños que puede causar nuestra información al alcance de la mano de un tercero. ¿Puede afectar la privacidad de una persona, a la cantidad de delitos que esta pueda ser víctima?

George Orwell¹ imaginaba, hace más de cincuenta años, un mundo en donde el "Gran Hermano" sabía todo, donde cada individuo era totalmente controlado y su privacidad simplemente era parte de un mundo ideal y solo para aquellos pocos que osaban imaginarlo.

A lo largo del trabajo intentaré mostrar cómo las nuevas tecnologías, la privacidad, y la seguridad, están ligadas de una u otra forma, cuáles son los roles que, a mi criterio, cumplen o pueden cumplir los diferentes actores que se presentan; y si todavía estamos a tiempo de vivir en un mundo diferente al que imaginaba el escritor en su libro, un mundo donde la privacidad del individuo, siga siendo un valor respetado y valorado.

¹ Escritor. Autor del libro "1984"

Seguridad y Privacidad

"Por primera vez se dio cuenta de que la mejor manera de ocultar un secreto es ante todo ocultárselo a uno mismo."

¿Qué se pretende de una red de información? ¿Qué se pretende de la sociedad de conocimiento? ¿Que sea segura? ¿Que tenga privacidad? ¿La seguridad implica privacidad? ¿O viceversa? Los términos seguridad y privacidad están íntimamente relacionados. Un usuario de las tecnologías de la información pretende (o debiera hacerlo) resguardar su privacidad a través del uso de las mismas.

La privacidad se define como el **ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión**².

La seguridad es la encargada de protegernos de dicha intromisión. La relación parece sencilla en cualquier ámbito. Por ejemplo, la privacidad de una persona cuando va a un baño público está resguardada en la seguridad que le brinda la cerradura de la puerta. Si dicha cerradura, o dicha puerta no existiera, el usuario no tendría privacidad.

La relación entre seguridad y privacidad es, entonces, una cuestión de equilibrios. Ambas fuerzas deben estar equilibradas para construir plataformas seguras y privadas. Sin embargo, la implantación de nuevas tecnologías de la información en la vida cotidiana, dificultan el mantenimiento de dicho equilibrio. Y esto se debe, no al factor privacidad, sino al factor seguridad.

La falta de concepción y elementos que posee un usuario para determinar si una tecnología es, o no, segura, es distante a los mismos elementos fuera del ámbito tecnológico. Cualquier individuo sabe si su casa está o no medianamente segura; pero este mismo, no tiene los elementos necesarios para definir si, por ejemplo, sus correos electrónicos están seguros, o no, en la plataforma donde se depositan.

Las consecuencias de dicho desconocimiento, por momentos, es la continua exposición de la privacidad de las personas, en plataformas que no la resguardan ni la segurizan. La segurización de las tecnologías debe implicar el resguardo de la privacidad de sus usuarios; caso contrario, el equilibrio ya mencionado entre ambos, se pierde y diluye de forma tal que el usuario es incapaz de conocer y decidir sobre sus cuestiones privadas.

² De la Real Academia Española - http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=privacidad

Web 2.0 y nuevas tecnologías en el siglo XXI

- "*¿Cuántos dedos ves aquí Winston?*"
- "*Cuatro*"
- "*¿Y si el partido te dijese que son cinco?*"

En los últimos años apareció en la red un nuevo concepto que trae aparejado mucho más que una simple definición, sino también nuevos modelos y paradigmas de comunicación: la **Web 2.0**.

La Web 2.0 es una redefinición de Internet que, en sus comienzos, fue una tecnología utilizada solo por grupos minoritarios, comenzando por el departamento de defensa de los Estados Unidos, y luego, expandiéndose a entes científicos, militares o gubernamentales. La llegada de Internet a la población en general, es mucho más reciente de lo que muchos jóvenes imaginan. Hace veinte años nada más, poca gente sabía de qué se trataba Internet. La masificación de los costos de acceso a Internet, no tiene más de diez años y probablemente la mitad si se habla de países ajenos al primer mundo. Con esta base, parece exagerado pensar que una tecnología que llegó masivamente a la población hace tan pocos años, se establezca en su versión 2.0. ¿Y la versión 1.1? ¿Por qué un salto tan grande? ¿Tantos fueron los cambios? Veamos...

La velocidad con la que creció Internet supera la imaginación de cualquiera y el sentido de la intuición; tanto por la tecnología, velocidad y cantidad de usuarios.

Internet nace hace menos de 30 años, a principios de la década del 80, a través de la red Arpanet (hoy Internet). Hasta ese entonces era una red cerrada desarrollada en los Estados Unidos y utilizada por el Departamento de Defensa de ese país. En el año 1984, la cantidad de usuarios ya superaba los 1,000. En 1989, ya superaba los 100,000 (cien veces más que 5 años atrás). En 1990, se creó el primer cliente Web. En 1992, el número de usuarios ya supera el millón. En 1997, el número de usuarios había crecido hasta veinte millones (20,000,000).

En 2007, diez años después, se calcula que hay más de quinientos millones de usuarios (500,000,000).

¿Cuántos usuarios del Internet de hoy, tomarán conciencia que el primer browser fue desarrollado hace tan solo 15 años?

Para resumir, **el número de usuarios de Internet aumentó en un 2500% (25 veces más) los últimos 10 años** y aumentó quinientas mil veces (500,000) su tamaño si tomamos como referencia 20 años atrás.

Con la masificación en la población, y el aumento en las velocidades, aparecieron en Internet nuevas formas de comunicación basadas en un principio fundamental de cambio: la interacción. El usuario hoy ya no es más un simple "cliente" de la Internet, que visita y consulta páginas web creadas y difundidas por los propietarios de los espacios. Hoy, el usuario es actor y creador de la Web. La interacción entre la web y los usuarios es la base de la famosa Web 2.0, la posibilidad de ser parte de ella, de modificarla y personalizarla a nuestro gusto.

Representantes de la Web 2.0

A pesar de ser un concepto, intentaré definir, según mi criterio, algunos modelos que considero ejemplificadores de la Web 2.0 y que, posteriormente, serán protagonistas de la relación entre la privacidad de los individuos y el uso de las nuevas tecnologías.

1. Blogs, Fotologs

Un blog es un sitio web donde uno o más autores publican artículos que son presentados de forma cronológica, apareciendo primero (más arriba) el más reciente. A pesar de que los blogs tienen más de diez años de vida, hoy se han popularizado de tal forma que muchos de ellos tienen la llegada y protagonismo de otros sitios de renombre. A través de Blogger y Wordpress, las plataformas más populares de publicación de blogs, se crean cientos de blogs cada día. Los blogs han evolucionado en la etapa 2.0 y hoy ya no son simplemente una publicación de artículos sino también un espacio de interacción con los usuarios, no solo a través de los comentarios, sino también a través de encuestas y posibilidades de participación de los lectores.

Junto con los blogs, surgieron los fotologs. A diferencia de un blog, un fotolog permite postear solo imágenes. Son utilizados por miles de usuarios en todo el mundo para compartir y publicar sus fotografías. Fotolog, la plataforma más popular de este servicio, ya supera los quince millones de usuarios y es uno de los veinte sitios con más tráfico en el mundo. Al igual que con los blogs, los visitantes pueden dejar sus comentarios en cada imagen.

2. Redes Sociales

Las redes sociales en Internet, son sitios donde nuclear la actividad de un usuario web

respecto a su contactos y amigos. La idea básica es la posibilidad de unir tus contactos a tu red y que ellos a su vez creen sus redes con sus amigos y su entorno. Las características que se ofrecen son la posibilidad de compartir tu perfil, tu libreta de direcciones, conocer nuevas personas a través de tus contactos y mantener una actividad social en la red.

Los sitios más populares de redes sociales son My Space (además de popular, de los primeros en salir a la web) y Facebook; aunque existen otras plataformas similares.

Actualmente las redes sociales se han integrado con otros servicios de la web y los usuarios poseen cada vez más servicios vinculados, como el correo electrónico y todo tipo de servicios web a los que se encuentren suscriptos, integrados en las plataformas ya mencionadas de redes sociales.

A pesar de ser estos sitios los denominados redes sociales por excelencia, son considerados también redes sociales otros espacios: los mismos blogs por ejemplo, o también la Wikipedia, una enciclopedia on-line en donde cualquier usuario puede participar y editar un contenido.

3. Mensajería

La mensajería instantánea no es un representante de la Web 2.0. Sin embargo, la evolución en las velocidades de Internet ha permitido utilizar nuevos servicios y usos asociados a la mensajería instantánea.

Por un lado, nuevas tecnologías permiten comunicación no solo de texto, sino también de voz y video a través de prácticamente cualquier cliente de mensajería. Los más populares, como MSN o Yahoo Messenger lo permiten y otras tecnologías como Skype incluso se caracterizan por su uso en transmisión de voz y video.

Además, la mensajería instantánea ya no es solo una herramienta de entretenimiento personal sino que a través de ella se generan negocios o se dictan cursos. Los cambios en la tecnología no fueron tantos pero sí las formas en las que se las utilizan con las nuevas velocidades de transmisión.

4. E-Commerce

Según el criterio de muchos especialistas, el E-commerce es la gran revolución y el gran cambio en los modelos de negocio de los últimos tiempos.

Se define de forma simple: es la compra-venta de servicios y/o productos a través de medios electrónicos.

Dentro del E-commerce se puede mencionar, no solo los sitios de venta directa a través de Internet, sino también nuevos modelos como las subastas (Ebay), la posibilidad de utilizar los bancos a través de Internet o el pago y/o alquiler de servicios a través de la web.

Por citar solo algún ejemplo, un usuario puede hoy en día, comprar un boleto de avión por Internet y acercarse a la empresa solo el día del viaje.

Estos, son solo algunos actores involucrados en un concepto mucho más amplio del que se presentó. La lista es extensa, y se presentaron solo los elementos y ejemplos más importantes. My Space y Facebook son solo dos de las redes sociales más populares; se podrían mencionar muchas más, como por ejemplo Twitter, un espacio donde la gente publica breves oraciones sobre su vida; quedando así publicado en Internet todo lo que una persona realizó en su jornada.

No solo los nuevos modelos que se listaron son los protagonistas, sino también antiguos modelos que han tomado nuevas formas y nuevos usos: el correo electrónico o los teléfonos celulares son ejemplos de ello. Hace no más de diez años, un usuario con acceso a Internet bajaba sus correos una o dos veces al día y, probablemente, contaba con los dedos de las manos la cantidad de mails que descargaba. Hoy, un usuario deposita en el correo electrónico gran parte de sus relaciones personales y laborales, probablemente sin descargarlo y borrarlo de los servidores web, sino utilizándolo directamente desde un servidor de terceros. Igualmente, un teléfono celular, antes un simple dispositivo para realizar y recibir llamadas de voz, es hoy una herramienta que nos permite intercomunicarnos por múltiples tecnologías, no solo de voz, sino también de video o de datos. Cada vez es más común, incluso, utilizar el teléfono para acceder a las cuentas bancarias y realizar transacciones desde allí.

No solo la masificación de Internet implica la relación cotidiana entre los usuarios y las nuevas tecnologías. Al igual que con el teléfono celular, recién mencionado, existen otras tecnologías que cada vez más, están al alcance de los usuarios. Si una persona va al banco, es más probable que interactúe con una máquina que con una persona. Los bolsillos de las personas están llenos de tarjetas magnéticas, las llaves desaparecen y nuevas tecnologías de acceso aparecen y nos rodean: cámaras de seguridad, RFID, autos con nuevas tecnologías, bases de datos y aplicaciones ERP, entre otros&

Como se puede observar, en los últimos años se ha establecido una estrecha relación entre la vida cotidiana de las personas y el uso de tecnologías de la información que, sin duda alguna, han modificado la relación entre la seguridad, la privacidad y los usuarios.

Jaque a la identidad

Maldad humana un ideal por el que convenía luchar, sino un peligro que había de ser evitado."

Todas las tecnologías explicadas en la sección anterior, forman en mayor o menor medida parte de la vida de cualquier persona del mundo con estabilidad económica media. Incluso muchas de ellas forman parte de la cotidianeidad de estas personas y son vistas con total normalidad por estos; no como una evolución de Internet, como fueron presentadas en el presente.

Sin embargo, la Web 2.0 presenta una característica más que fue omitida en la presentación anterior: **la continua exposición y utilización de nuestros datos personales**. Las redes sociales, por definición, implican depositar en una plataforma gran parte de nuestra información personal. Además, la regular utilización de otras tecnologías implican que el usuario esté expuesto constantemente a través de la entrega de datos personales a terceros.

Como consecuencia, nuevas amenazas han aprovechando la facilidad de las nuevas tecnologías para obtener información privada de los usuarios, y la costumbre del usuario de entregar esta información. El crecimiento del malware y el robo de identidad son dos amenazas a las que cualquier usuario medio de tecnologías está expuesto, aunque lamentablemente, muchos creen lo contrario.

El malware es una amenaza que acecha desde la década del 80. ¿Por qué entonces presentarlo como una amenaza del siglo XXI? Porque el software malicioso ha encontrado en las nuevas costumbres de los usuarios, oportunidades inmensas para mejorar, no solo el daño causado, sino también sus velocidades de propagación.

Entre las amenazas que se pueden mencionar figuran los virus, troyanos, gusanos, solo por mencionar los más populares. Navegar por Internet es un riesgo constante, especialmente en sitios que ofrecen pornografía, descargas gratuitas o cracks, entre otros. Un ordenador conectado a Internet, sin protección alguna, puede tardar tan solo unos minutos hasta que comience a infectarse de malware.

A la vez, técnicas de Ingeniería Social han avanzado profundamente y, a través del Spam y el Phishing, principalmente, el usuario se ve tentado constantemente a otorgar información personal a terceros.

Por otro lado, el robo de identidad se explota principalmente a través de las redes sociales y la web 2.0. El acceso a información personal a través de los perfiles de usuarios y la actividad registrada en plataformas sociales es muy común para conocer datos personales que permitan generar una nueva identidad.

Además, existen otros ataques de los que protegerse como las estafas en sitios web, el robo de contraseñas de cajeros automáticos o de información de acceso físico a cierta edificación.

Todo es riesgo con las nuevas tecnologías. Un nick en el cliente de mensajería ("Nos vamos de vacaciones!"), una foto subida a un fotolog, un mensaje publicado en un blog, todos son riesgos que atentan contra nuestra privacidad.

Como se puede observar, el usuario está expuesto de manera constante y amenazantes a los riesgos que atentan contra su privacidad. Ya no es una opción alejarse de estos riesgos, si se hace un uso medio de la tecnología.

Una amenaza sin riesgo: la pérdida de privacidad

Supongamos una persona profesional, por ejemplo un joven contador que busca trabajo, o que ya lo tiene. Su perfil profesional, sus notas académicas, su formación son intachables. Sin embargo, de un día para el otro lo echan de su trabajo, o simplemente queda eliminado de una búsqueda laboral sin explicación alguna. Quizás esta persona no sepa que sus fotos pasado en alcohol el fin de semana con sus amigos están dando vueltas por la web. O peor aún, quizás él mismo subió las fotografías y no imagina que las empresas pueden consultar en la web la información personal sobre sus postulantes o empleados.

Al mejor estilo orwelliano, los usuarios depositamos diariamente información personal en la web con la fantasía de que la web es un lugar seguro a la que acceden solo quienes nosotros querramos. Esbozar el perfil de un individuo, con sus principales datos personales, o incluso una fotografía, es tarea de niños para cualquier usuario que use medianamente bien un buscador.

La pérdida de la privacidad es un problema más allá de los riesgos directos asociados al malware o al robo de identidad como se presentó. La privacidad es un valor y el desconocimiento tecnológico permite que los usuarios dejen gran parte de su vida privada **publicada** en Internet. Apta para todo público. El resguardo de la privacidad es un principio que individualmente puede ser quebrantado solo por la información que cirula en Internet.

¿Quién es el responsable?

"En realidad, nada era ilegal, ya que no existían leyes."

Ramiro T. Robaron tiene 35 años. He aquí, un día de su vida.

Ramiro se levanta todos los días a la mañana y, luego de llevar a sus hijos al colegio, se toma su tiempo frente a la Pc para realizar algunas tareas cotidianas: primero chequea sus correos en su única cuenta Hotmail. Tiene un montón de correo no deseado e incluso algo de spam en su bandeja de entrada, que no fue filtrado por los sistemas. Ramiro se toma el trabajo de borrarlos todos, menos aquel que ofrecía un video de Fidel Castro bailando con Bush un baile ruso, ya que le resultó gracioso ver ese video que, finalmente, por un problema en su compu, no lo pudo descargar; algo le impedía bajar un video y lo mandaba a una página rara, tenía que llevar su computadora a reparar. El otro correo que le resultó interesante a Ramiro, era aquel que pedía una ayuda para un chico Nwaka Zamir, que vivía en el Congo y que tenía una enfermedad terminal llamada IneniusSocialibis, que lo acechaba hace años. El correo pedía, encarecidamente, si alguien podía donar un riñón y tres kilos de morcilla para evitar la muerte de este inocente pequeño de cinco años. Ramiro reenvió el correo a sus casi 200 contactos y, agregó su comentario en la parte superior del correo (arriba de todos los correos a los que ya había sido enviado anteriormente): "esto no es una pavada, es una cuestión de vida o muerte". Terminada su tarea de chequear correos, Ramiro se dispuso a marcharse al trabajo, aunque antes, tenía una reunión en un bar con un cliente. Cuando llegó al bar, el cliente aún no había llegado, así que Ramiro aprovechó para conectarse al Wi-Fi del lugar y verificar algunas cuestiones de sus cuentas bancarias desde el Home Banking que a él le resulta tan cómodo ("No puedo creer que ya casi ni voy al banco" le dice a sus amigos). Previo a ello, como no podía conectarse a la red, desactivó su antivirus ya que suponía que por ahí estaba el problema y, finalmente pudo navegar por Internet y aprovechó para subir unas fotos de su hijita menor de dos años a un fotolog que había creado para que todos sus familiares pudieran ver las fotos de su familia, sin necesidad de enviarlas por e-mail.

Antes de que llegue por fin su cliente, su mujer lo llamó del trabajo y le pidió que le recuerde la contraseña del cajero, a lo que Ramiro respondió a viva voz: "Querida, ¿no te acordás la contraseña? es 1811, ¡como mi cumpleaños!". Al colgar, su cliente ya se estaba sentando en la mesa.

Más tarde Ramiro llegó a su trabajo, y antes de empezar, aprovechó para leer los diarios por Internet y divertirse un rato con unas nuevas Toolbars que le instaló a su Internet Explorer 7. Además, pudo cargar sus actividades en Twitter ("reunión en un bar con un cliente" - "ya estoy en el trabajo hasta las seis de la tarde") y ver los mensajes que sus amigos y contactos varios (más de 200 también) le dejaron en su FaceBook.

Pasó la mañana de reunión en reunión y cuando salió vio que tenía mensajes en su casilla de voz del celular. Discó el número correspondiente, su contraseña (1234) y escuchó que su mujer le pedía que en cuanto pueda se conectara al MSN, que tenía que decirle algo. Así lo hizo, pero antes de chatear con su mujer ya tenía más de 5 contactos saludándolo (sobre los 150 que tenía en su lista) entre los que figuraban uno de sus hijos, un compañero de trabajo, dos amigos del chat (no recuerda donde los conoció) y una chica que lo estaba invitando a ver por la Webcam. Pensó que si estuviera en su casa podría verla pero que ahora, en el trabajo, no podía, y además debía ver qué necesitaba su mujer. El problema de su esposa era que no había podido utilizar la tarjeta bancaria y se había bloqueado su contraseña. Ramiro no podía entender cómo no pudo sacar plata del cajero pero ella argumentó que incluso le pidió ayuda a una persona que estaba en la cola y que tampoco había podido ingresar la contraseña.

La tarde de Ramiro terminó sin problemas y se marchó a su casa. Cuando llegó saludó a sus hijos. Uno de ellos, el mayor de 15 años (el mismo que lo había saludado en el Messenger) seguía en la Pc conectado al chat. Le preguntó: "Ey pá, ¿vos cuántos contactos tenés en el Messenger?". "No se hijo, unos 150, 200... no sé" dijo Ramiro, a lo que su hijo se rió y le dijo: "Ja, yo ya tengo más de 400 y soy el que más tengo de mi curso". El padre no entendió muy bien por qué los chicos en la escuela competían a ver quién tenía más contactos pero supuso, que era tan solo un juego de niños.

El día de Ramiro no terminó muy bien. Cuando fue a saludar a su mujer se encontró con una caja abierta arriba de la mesa y adentro, había lo que parecía un DVD. Ramiro recordó que había comprado en un sitio de subastas un lector de DVD por tan solo \$120 y por fin estaba contento de que su encomienda estuviera con él. Sin embargo, su mujer le amargó la noticia: "Te informo que no funciona, yo te dije que no le podías comprar algo así a cualquiera, ¡nos robaron más de cien pesos!". Ramiro intentó tranquilizarla diciendolé que iban a reclamar y todo iba a estar bien pero su mujer le informó que ya había hecho el reclamo y le había informado que, como era un producto en oferta, no se podían realizar reclamos.

Antes de acostarse amargado, Ramiro decidió darse una vuelta por la Pc para dejar durante la noche descargando películas en su cliente P2P; pero al prender el ordenador un mensaje ocupó su pantalla: "Su Pc puede estar en peligro. Es muy probable que estalle en pedazos. Haga clic aquí para instalar la solución en

seguridad que estaba esperando de forma gratuita por cinco años.” Ramiro agradeció que su antivirus (el mismo que había desactivado por la mañana) le avisara de tal peligro e intentó instalar la aplicación ofrecida. Sin embargo, luego de descargar y ejecutar los archivos indicados, el mensaje de alerta seguía apareciendo.

Al igual que por la mañana pensó: “Tengo que llevar mi computadora a reparar”.

La historia de Ramiro T. Robaron no es muy distante de la de muchos de nosotros. La mayoría de las herramientas y plataformas mencionadas son utilizadas masivamente y los problemas que tuvo Ramiro, fueron tan solo algunos ejemplos de los miles de problemas con los que se encuentra cualquier individuo diariamente en su relación con las tecnologías.

¿Es Ramiro un irresponsable? ¿Cuán expuesto estaba Ramiro a cualquiera de las amenazas indicadas anteriormente?

Tomaré tan solo un ejemplo: Ramiro utiliza como contraseña en su teléfono celular el famoso '1234' que viene por defecto. Cualquier profesional en seguridad sabe que las contraseñas se pueden hacer expirar. Según ese criterio, la compañía telefónica es responsable por no obligar a sus usuarios a modificar su contraseña. Sin embargo, Ramiro no queda exento de culpa ya que muchos usuarios saben que deben hacerlo, y de hecho modifican su contraseña al recibir un nuevo teléfono.

La responsabilidad en materia de seguridad y privacidad es compartida. Los usuarios no quedan exentos, pero las compañías deben tomar responsabilidad por la seguridad de sus usuarios y aquellas plataformas que concentran datos personales deben ser responsables en el uso de dicha información.

La legislación en materia de privacidad tecnológica es pobre en la mayoría de los países. Unas pocas organizaciones bregan por los datos personales de los usuarios pero sus denuncias no llegan a un final concreto en la mayoría de los casos.

La responsabilidad por la seguridad y la privacidad de los datos personales debe ser compartida entre los estados a través de la legislación; las empresas a través de transparencia y responsabilidad social; y los usuarios a través de acciones responsables en el uso de las tecnologías.

Dos opciones: inclusión o privacidad

"Si los hechos demuestran otra cosa,
habrá que cambiar los hechos."

A pesar de las responsabilidades conjuntas presentadas en la sección anterior, la realidad indica que:

- la legislación en materia de protección de datos personales es pobre en la mayoría de los países e incluso las barreras de legislación a través los países es aún más pobre.
- las empresas proveedoras de tecnología no son transparentes respecto al uso que hacen de los datos que los usuarios depositan en sus plataformas y existen importantes denuncias respecto al almacenamiento de datos personales.
- las amenazas a la que los usuarios son expuestos aumentan exponencialmente cada día aprovechando el contexto presentado en los ítems anteriores.

Entre el contexto ideal y el contexto real las distancias son lo suficientemente grandes como para intentar vivir en el primero. ¿Cuál es el mundo ideal? El de Ramiro, el de confiar y utilizar las herramientas indiscriminadamente, inspeccionar cada herramienta nueva que aparezca y desconocer totalmente los conceptos básicos de funcionamiento de las tecnologías e ignorar prácticamente cualquier amenaza a la que uno está sometido. Este es el mundo de la inclusión, utilizando todas las herramientas que aparecen en el mercado, las que usa nuestro contexto, las que "queda bien" usar.

Pero existe otra opción: la privacidad. Utilizar la menor cantidad de herramientas posibles es una opción y, con seguridad, resguarda mucho más la privacidad del usuario que la anterior. La responsabilidad del usuario radica en replantearse ante cada herramienta tecnológica que esté a la vista si es o no necesario hacer un uso de ellas, si son prescindibles.

En resumen, el usuario posee hoy infinidad de herramientas tecnológicas con las que interactuar en su vida cotidiana. Estas plataformas poseen mayor o menor seguridad respecto a las amenazas que se presentan y el resguardo que se hace de los datos personales de los usuarios. El usuario puede elegir entre dos opciones: utilizar todas las herramientas y estar incluido en la sociedad, con sus modas y costumbres respecto a la tecnología; o bien, asegurar su privacidad más allá de las costumbres, rechazar las plataformas en las que no se confíe, utilizar la menor cantidad de herramientas nuevas y mantener modelos viejos que aseguran mejor la privacidad de nuestros datos.

Conclusión

La tercera opción: uso responsable de las tecnologías

"Hasta que no tengan conciencia de su fuerza, no se rebelarán, y hasta después de haberse rebelado, no serán conscientes. Éste es el problema."

Adrede omití esta opción en la sección anterior, ya que frecuentemente la presentación de los hechos mencionados generan en el usuario la sensación de que la única forma de mantener la seguridad es, o bien siendo un paranoico, o bien resignarse a los problemas y riesgos que implican las nuevas tecnologías respecto a la privacidad.

Incluso profesionales en seguridad caen en el simplismo de exigir al usuario, como única medida de resguardo, niveles de paranoia cuya probabilidad que el usuario comparta y realice tienden a cero.

La tecnología rompe barreras elementales de seguridad. Cualquier persona al salir a la calle, conoce las amenazas y riesgos a los que se enfrenta en mayor o menor medida. Un usuario usando un ordenador con Internet, conectándose a un Home Banking o cargando información privada en una red social, probablemente desconozca las amenazas más elementales a las que se enfrenta, ni el funcionamiento básico de las tecnologías que está utilizando.

Y a mi criterio, esa es la solución: usuarios concientes y capacitados. La educación tecnológica es el principio del **uso responsable de las tecnologías**. Culpar al usuario es el camino más simple e indicarle la exclusión del sistema tampoco es viable. ¿Por qué un usuario cuando se muda a una casa nueva, acostumbra cambiar la cerradura y no hace lo mismo cuando recibe una contraseña por defecto? La educación desde la infancia y la concientización constante es el camino.

Las responsabilidades deben recaer sobre todo el espectro tecnológico, incluido el usuario, pero con una gran responsabilidad en los profesionales en seguridad a través de la capacitación y el asesoramiento por una educación tecnológica; el estado, a través de la legislación y la acción educativa en los medios formales; y las empresas de tecnología, a través de un mayor compromiso con la privacidad de sus usuarios y políticas claras de configuraciones seguras más allá de la usabilidad que se pretenda dar al usuario.

De una forma u otra, si el usuario está capacitado y es conciente ya es elemento suficiente para poder hacer un uso responsable de la tecnología.

¿Qué es un uso responsable de la tecnología? Es hacer una lectura crítica de las plataformas que utilizamos, no solo web sino cualquier componente tecnológico. Es conocer las amenazas y riesgos a lo que nos enfrentamos y permitir al usuario alejarse de la paranoia que puede caracterizarnos a quienes trabajamos en seguridad, permitiéndole configuraciones seguras y un uso responsable.

No es la intención del presente, negar que existen sitios a los que es altamente recomendable no acceder ni utilizar sus servicios. Pero muchas de las tecnologías que utilizamos hoy en día es muy complejo pretender que un usuario prescinda de ellas.

Obviamente sería mucho más simple explicarle a un usuario que no tenga tarjetas de crédito ni débito; o que no utilice un servicio como Facebook o My Space.

Sin embargo, considero que el mayor problema no está en la utilización de los mismos, sino en el desconocimiento y en el uso "a ciegas" de dichas tecnologías. A través de la concientización se puede lograr que un usuario haga un uso razonable en cuanto a los riesgos de alguno de los servicios mencionados.

Luchar por un uso responsable de la tecnología no es simple y requiere, como en muchos aspectos relacionados a la seguridad, de un fuerte compromiso de muchas partes con la columna vertebral basada en la concientización.

Me considero un usuario responsable de las tecnologías que, aunque por momentos paranoico, intento comprender y securizar las plataformas y las configuraciones pero, en la medida de lo posible, no rechazarlas.

De esta forma, encuentro el equilibrio que, intencionalmente antes planteaba como imposible, entre la inclusión y la privacidad; y entre los factores con los que comienza el presente: el equilibrio entre seguridad y privacidad.

Glosario

- **Gusano:** Son archivos maliciosos, al igual que un virus pero sin la capacidad de auto reproducción. su transmisión es a través del correo electrónico o descargas web pero no de forma automática.
- **Home Banking:** Es la plataforma para realizar tareas bancarias a través de Internet. Según la entidad financiera, se pueden realizar mayor o menor cantidad de operaciones.
- **Malware:** Acrónimo en inglés de 'Malicious software' ('Software malicioso'). Es cualquier programa o archivo que es dañoso a un usuario de ordenador. Así, malware incluye virus informáticos, gusanos, caballos de Troya o spyware.
- **Troyano:** Son archivos maliciosos que simulan ser indefensos y esconden su identidad, simulando ser aplicaciones inofensivas para lograr así que el usuario ejecute el archivo con la amenaza.
- **Virus:** En ordenadores, un virus es un programa que se autoreproduce y cuyos fines son maliciosos. Los virus pueden ser transmitidos como adjuntos de un correo electrónico o en un archivo descargado, o estar presentes sobre un disquete o CD.
- **Wi-fi:** Acrónimo en inglés de '*Wireless-Fidelity*'. Son un conjunto de normas y estándares para redes inalámbricas. El término es utilizado frecuentemente para referirse a cualquier red inalámbrica doméstica de conexión.

Bibliografía - Weblografía

Definiciones

- Real Academia Española
<http://www.rae.es/>
- Wikipedia
(en inglés) <http://www.wikipedia.com/>
(en español) <http://es.wikipedia.org/>

Papers

- Seguridad y privacidad para el ciudadano en la era digital posterior al 11 de Septiembre: una visión prospectiva
<http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/Libe%20IPTS%20study%20Executive%20Summary%20spanish%20version.pdf>

Libros

- DE UGARTE, David. El poder de las redes
http://www.deugarte.com/gomi/el_poder_de_las_redes.pdf

Noticias

- Segu-Info
<http://www.segu-info.com.ar/blogger/>

Todas las noticias y delitos mencionados en el presente, forman parte del blog de seguridad de Segu-Info, principal fuente de inspiración para las ideas presentadas en el paper; salvo las que se mencionan a continuación:

- Fotolog supera los 15 millones de miembros
<http://www.diarioti.com/gate/n.php?id=16838>
- El crecimiento de Internet
<http://unmundobinario.wordpress.com/2007/11/27/el-crecimiento-de-internet/>
- ¿Bebiste ayer? No lo muestres en Facebook
<http://www.identidadrobada.com/site/index.php?idSeccion=19&idNota=1400>
- Redes Sociales por Enrique Dans
<http://www.enriquedans.com/?s=redes+sociales&x=0&y=0>

Sitios web citados

- Blogger
<http://www.blogger.com/>
- Wordpress
<http://www.blogger.com/>
- My Space
<http://www.myspace.com/>
- Facebook
<http://www.facebook.com/>
- MSN
<http://latam.msn.com/>
- Yahoo Messenger
<http://es.messenger.yahoo.com/>
- Skype
<http://www.skype.com/>
- E-Bay
<http://global.ebay.com/>

Citas

- Wikiquote
<http://es.wikiquote.org/wiki/1984>