Sonría, está siendo observado

Nuestras acciones al usar tarjetas de crédito, enviar mails, chatear, registrarse como usuarios en redes y servicios, van dejando un rastro o "sombra" digital que puede ser usado para atentar contra nuestra privacidad. La velocidad con la que avanza la revolución digital es mucho mayor que la velocidad con la que avanzan los mecanismos para proteger los datos personales y financieros.

En el mundo actual, donde nuestros datos son fácilmente accesibles, debemos aprender nuevos hábitos de protección y a utilizar herramientas informáticas y jurídicas, que aunque escasas, nos pueden igualmente resultar útiles.

POR: CARLOS PACHECO Y LUCÍA CUOZZI

Un profesor universitario uruguayo recibió un mail que lo reconfortó. Le escribían desde una universidad peruana y le decían que lo habían elegido para entregarle un Doctorado Honoris Causa. Elogiaban sus trabajos y destacaban los méritos por los que lo habían elegido. También le pedían que confirmara la recepción del mail y le decían que en futuras comunicaciones le indicarían los pasos a seguir.

Este profesor tenía unos 50 años y había trabajado e investigado de forma muy intensa por más de 25 años. Sentía que no había sido reconocido en su país como lo merecía. Ahora le llegaba el reconocimiento, pero como siempre, pensó, llega desde afuera. Contestó el mail y agradeció por su elección para tan honrosa distinción.

Una semana después le enviaron otro mail, con detalles concretos. Le explicaron cómo iba a ser la ceremonia, el día, la hora, quiénes iban a hablar. Estaba programado para llevarse a cabo en tres semanas. Luego le explicaron que estaba todo coordinado para su traslado y alojamiento. Le informaron del probable vuelo en que viajaría y del hotel en que se alojaría. Le pedían que confirmara su disponibilidad para la fecha mencionada. El profesor se dijo a sí mismo "me las voy a arreglar y allí voy a estar". Confirmó su presencia. Le dieron la dirección web de la Universidad. Ingresó. Se trataba de un sitio web institucional, con información muy básica, pero allí confirmó los datos que le habían enviado por mail.

Pocos días después recibió un nuevo mensaje, que incluía una agenda con horarios de la ceremonia, reuniones con colegas, una entrevista para un medio radial y datos concretos sobre la reserva de avión y del hotel. El intercambio de mails continuó en los días siguientes y cuando faltaban 10 días para la ceremonia, recibió un mail en el que le explicaban que había surgido un problema. Se estaba realizando la auditoría anual y el desembolso que debía realizar la Universidad para pagar los gastos de viaje y traslado se iba a demorar por unos días. Le explicaron que la mejor solución era que él pagara los gastos y que le serían restituidos en cuanto llegara al país. De lo contrario, lo más probable era que se procediera a postergar la ceremonia. Por la agenda de eventos de la Universidad, tendría que realizarse un año después. El mensaje no le cayó muy bien al profesor, pero estaba muy entusiasmado con el reconocimiento que iba a recibir y temía que si se confirmaba la postergación finalmente no se lo dieran. "Una oportunidad como esta se da una sola vez en la vida", pensó. Escribió que no tenía problema en facilitar las cosas para que todo continuara tal como había sido planificado. Le contestaron que estaban muy agradecidos por su gesto y que se quedara tranquilo que el dinero le sería reembolsado. Le indicaron que debía ingresar al sitio web de una agencia de viajes, le dieron un nombre de usuario y contraseña.

El profesor ingresó al sitio con el usuario y contraseña y apareció su nombre con la descripción del ticket de vuelo y la reserva de hotel. Ingresó sus datos personales, los datos de su tarjeta y pagó US$800. Luego escribió a la universidad y les confirmó que había realizado el pago.

No le contestaron.

Al día siguiente volvió a escribir.

No le contestaron.

Intentó ingresar al sitio web y sólo recibió un mensaje que decía "servidor no encontrado".

Nuestra sombra digital

Este caso es real. Hay algunos detalles cambiados, para proteger la identidad del afectado. Se trata de un profesor uruguayo que fue estafado mediante un método que se conoce como phishing o robo de identidad. Le hicieron creer una determinada situación (en este caso un reconocimiento, en otros casos problemas con una cuenta bancaria o una tarjeta), lo hicieron ingresar en un falso sitio web, le robaron US$800 y sus datos personales y financieros.

Lo interesante de este caso es que los estafadores aplicaron diversas metodologías de apropiación de información. Localizaron a un profesor universitario, se cercioraron que ya tenía una larga carrera, pero que no había recibido reconocimientos. Se puede decir que

Cómo proteger nuestros datos personales

Gabriel Barandiarán, Director de Causa Común, realizó las siguientes recomendaciones para proteger nuestros datos.

1. Datos para encuestas y sorteos.
"Uno no tiene que entregar los datos personales si no hay un motivo por los que deba darlos. Si viene alguien y nos dice que está haciendo una encuesta y nos pregunta demasiados datos personales probablemente esa persona está consiguiendo información para dársela a un vendedor. Después nos llaman y nos dicen que nuestro nieto o hijo ganó un premio que debemos retirarlo en tal lugar y ahí nos quieren vender algo. El tema es ser muy concientes de este hecho cada vez que llenamos un cupón o damos datos. No debemos tomarlo a la ligera".

2. Tarjetas de crédito.
"Las tarjetas son soportes de información por lo que hay que tener cuidado de no darla por teléfono, no darla por Internet salvo en sitios con mecanismos seguros. Hay que manejarse con mucho cuidado. Nunca se deben dar los pin".

3. Internet y el robo de identidad.
"Respecto a Internet tenemos que estar informados de las formas de estafas más comunes. Si me mandan un mail pidiéndome datos para actualizar la base de mi banco puedo estar en riesgo y es mejor llamar al banco y confirmar. Tenemos que tener en cuenta que en Internet estamos expuestos al robo de identidad y debemos saber que esto puede tener consecuencias muy serias. El robo de identidad más fácil que ocurre en Uruguay es cuando perdemos la cédula. Hasta hace muy poco, cuando uno la perdía, si el que la encontraba sacaba un crédito, lo tenía que pagar uno".

4. Enseñarle a los niños.
Hay que hablar de este tema con los niños, hay que incluir el tema de los riesgos ya que estamos entrenándolos en la era digital y muchas veces son los niños los que dan datos de la familia sin saber lo que están haciendo.

5. Empresas.
Las empresas que sufrieron algún tipo de fraude, o a las que fueron perjudicadas con la falsificación de su página web y eso se utilizó para pedir datos a sus clientes, deben informarlo. Muchas veces no lo hacen para no mostrar que fueron vulnerables pero si no informan terminan siendo cómplices de lo que están tratando de evitar. Hay que reconocer el problema y buscar la solución.

buscaron un cierto perfil de persona, y descubrieron su vulnerabilidad. Para ello utilizaron datos dispersos que estaban en Internet. Luego montaron una maniobra que incluía un sitio falso de una universidad y un sitio falso de una agencia de viajes. Ejecutaron la estafa, robaron su identidad y se esfumaron.

"Nosotros permanentemente vamos dejando rastros de nuestra información, lo que se llama sombra digital, ahora esa sombra puede afectarnos en distintas medidas, porque puede ser utilizada en nuestra contra", señaló el Cr. Gabriel Barandiarán, Director de Causa Común, organización no gubernamental de defensa de los consumidores, y ex diputado por Montevideo (1995-1999).

Los atentados a la privacidad y los crímenes informáticos cada vez afectan a más uruguayos. Cada vez hay más casos dentro del territorio uruguayo, y también hay víctimas de delincuentes internacionales que utilizan los sistemas financieros y de comunicación globalizados.

La privacidad en tiempos digitales

"Debemos partir de qué se entiende por privacidad. En general, la doctrina enseña que se trata de una noción más abarcativa que la tradicional de intimidad", señaló el Dr. Carlos Delpiazzo, experto en informática jurídica, ex Ministro de Salud Pública (1991-1992) y senador en 1998. "Mientras que la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, la privacidad constituye un conjunto, más amplio, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado y, por ende, a que no sea conocido sin su consentimiento expreso".

Uruguay ha tenido varias etapas en lo que respecta a la privacidad de las personas, que dependen mucho de la actividad económica, afirmó Barandiarán. "Las prácticas hoy más comunes son algunos problemas con las tarjetas de crédito, las tarjetas de débito en los cajeros automáticos, las lla-

Preguntas frecuentes

En los últimos años se han dado algunos casos de atentados o presuntos atentados a la privacidad que han generado dudas sobre su gravedad e incluso si pueden considerarse delitos. El Dr. Carlos Delpiazzo respondió a algunas de las preguntas más frecuentes. Las respuestas son generales y deben ser tomadas como un simple acercamiento a cada una de las situaciones.

Un director o dueño de empresa, ¿puede abrir los mails de sus empleados? ¿en qué caso?
El acceso por el empleador al correo electrónico del trabajador ha sido abordado reiteradamente, en distintos supuestos, por la Justicia laboral. Los fallos han tenido en cuenta si el correo electrónico respectivo era de la empresa o del trabajador, si existían o no reglas de conducta predeterminadas acerca del uso del correo electrónico en la empresa, si el mismo fue usado lícita o ilícitamente por el trabajador, etc.

Reenviar a otras personas un mail que recibimos de otra persona, ¿puede ser un delito?
Los datos personales de terceros accedidos en el marco de una determinada relación, no pueden ser usados con fines distintos de acuerdo a los principios que recoge nuestra ley Nº 18.331, a menos que se cuente con el consentimiento expreso del interesado.

La copia de información empresarial. ¿En qué casos es un delito?
La copia de información empresarial puede constituir una maniobra de competencia desleal. Si es realizada por un trabajador, puede implicar notoria mala conducta habilitante de su despido sin indemnización.

Utilizar el mail de otra persona para enviar mensajes en su nombre pero sin contar con su autorización. ¿En qué casos puede ser un delito? ¿En qué casos no?
Utilizar el mail de otra persona para enviar mensajes en su nombre es siempre una conducta prohibida.

Delpiazzo explicó que "La Sección Delitos Informáticos del Departamento de Delitos Complejos de la Dirección de Investigaciones de la Jefatura de Policía de Montevideo ha desarrollado medios para la identificación de los mails anónimos o, más precisamente, para la determinación del origen de un mail lesivo. Cuando dicho medio se utiliza para cometer un delito, la pena aplicable es la que corresponde al comportamiento típico realizado y no depende tanto del medio empleado".

¿Lo tiene que saber el empleador?

El Cr. Gabriel Barandiarán explicó que es muy importante "que la persona pueda saber que hay determinada información que está bien que la brinde, pero para algunos casos, no para todos".
En los siguientes tres casos, Barandiarán menciona situaciones en las que las personas pueden no ser elegidas para un empleo porque el empleador accedió a información personal que el aspirante tiene derecho a mantener en su privacidad.

Una persona con SIDA. "Es razonable que si una persona tiene SIDA esta información aparezca en su ficha médica porque es algo que debe conocer el médico que lo está tratando. Pero ese dato no tiene porque tenerlo un empleador".

Personas que hicieron paros. "En un momento en Uruguay existió un caso de venta de datos de personas que habían realizado paros. Muchas de las personas que estaban en esa base de datos no eran tomados en los empleos y no se daban cuenta por qué. No sabían que era porque su nombre estaba en dicha base de datos. Ese es un dato que no tiene por qué estar en manos de un empleador y mucho menos sin el consentimiento de la persona afectada".

Historial crediticio. "Es razonable que tu historial de créditos sea consultado por una empresa a la que vos le pediste un crédito, pero no te la tiene porque consultar alguien que te va a tomar como empleado. Deberíamos preguntarnos si es socialmente aceptable que por ejemplo se le niegue el trabajo a una persona porqué se atrasó en el pago de una radio".

madas telefónicas, que pueden robar datos personales, porque hacen falta prácticas comerciales sanas que protejan la identidad de los clientes. Debemos decir que estas prácticas son alentadas además por la falta de conciencia de la población de que es necesario proteger estas cosas".

El efecto Internet

El deslinde entre lo público y lo privado siempre es delicado de definir y más aún con la aparición de las nuevas tecnologías, opinó Delpiazzo. "Las posibilidades invasivas de lo privado se multiplican. Y tales posibilidades no sólo pueden constituir delitos sino que en la mayoría de los casos pueden ocasionar daños no reprimibles penalmente sino reparables civilmente, por ejemplo".
Según Barandiarán "a veces no nos damos cuenta que estamos en el medio de una revolución". El avance de la técnica, afirmó, permitió un nuevo manejo de la información personal. "Hablo de datos relevantes de las personas, eso siempre existió, lo que pasa es que hoy con el avance de la informática y de Internet lo que antes llevaba más trabajo y tiempo ahora no implica casi tiempo ni esfuerzo". En su opinión la técnica ha avanzado más rápido que nuestra propia comprensión del problema. "Hoy se indexa una cantidad de datos por la cédula, pero también utilizando simplemente el nombre y apellido. Alcanza con ver Google. Hay mucha gente que pone tal vez demasiada información en sus perfiles de las redes o en los comentarios de blogs. Una vez que dejó información en Internet ya no es dueño de ella. Si la gente supiera de la cantidad de información que se puede llegar a obtener de una persona, se sorprendería".

La ley

Según Delpiazzo la legislación uruguaya sobre protección de datos personales es avanzada. No obstante, su alcance está limitado por otras leyes que perforan esa protección, "como es el caso de las normas que atribuyen facultades inquisitivas exageradamente amplias a la Administración fiscal, por ejemplo". Delpiazzo es un destacado docente, con años de ejercicio y

Cr. Gabriel Barandiarán, Director de Causa Común, organización no gubernamental de defensa de los consumidores.

Dr. Carlos Delpiazzo, experto en informática jurídica.

enseñanza en la materia. En su opinión, si se tiene en cuenta "que la Informática es una ciencia joven y que el Derecho que a ella refiere lo es más, Uruguay es un país relativamente avanzado en el contexto comparado, aún cuando su legislación en la materia ha sido tradicionalmente minimalista, es decir, que ha procurado atender a los problemas planteados por la Informática sin caer en la casuística exagerada o en la hiper-regulación que se advierte en otros países en algunas áreas". Destacó que se van a cumplir 25 años del inicio, en 1984, de los cursos de Informática Jurídica en la Facultad de Derecho de la Universidad de la República. Entre los aspectos más sensibles, destacó que de cara al futuro "es necesario avanzar en lo que refiere a la adecuada tutela de los derechos humanos frente a las nuevas tecnologías y, en particular, para que la brecha tecnológica (entre quienes tienen acceso a esas nuevas tecnologías y quienes no lo tienen) no implique un nuevo factor de fragmentación social".

Apuntó que si se observan las sentencias publicadas en el anuario de "Derecho Informático", y se hace una compulsa se advierte que los temas más recurrentes son los referidos a la violación de la propiedad intelectual (de programas y otras creaciones informáticas), el uso indebido del correo electrónico, la estafa mediante el empleo del computador o de Internet, las maniobras con tarjetas magnéticas, la violación de secretos, falsificaciones, y similares. Señaló que "la mayor cantidad de jurisprudencia en materia informática no es penal sino civil, laboral y contencioso administrativa".

Infotráfico

"En Causa Común utilizamos el término de 'infotráfico', que es el tráfico de información personal sin autorización de las personas dueñas de esos datos, y muchas veces en contra de esas personas", explicó Barandiarán. "La información de las personas, en general, debería ser privada, no como en el caso de información del Estado o de una empresa, que en general, debería ser pública".

A Barandiarán le preocupa particularmente el tema de los catastros personales, de información crediticia. "Mientras se mantenga como información crediticia no hay problema, si yo pido un crédito es razonable que esa empresa consulte mi información crediticia, pero creo que nadie debería mirar esa base de datos si yo no le vine a pedir el crédito, y mirar esa información es una práctica común". En su opinión la información de las personas no debería poder venderse ni comprarse sin la autorización de la persona a quien pertenece.

Cuidado con el phishing

El llamado phishing o robo de identidad es un engaño que se ha popularizado últimamente y que puede tomar por sorpresa a muchos.

El esquema básico del phishing es el siguiente:

1. Le envían un mail a una persona, en la que le plantean alguna situación. Puede ser una situación presuntamente positiva, como por ejemplo un premio o una distinción, o más comúnmente le indican que hay un problema, o sea intentan asustar a esa persona. Por ejemplo, en el asunto dice "Asia Lotto International Promotion" (un premio), o "eBay Unpaid Item Dispute for Item #290250074158– Response Required" (se hacen pasar por eBay y mencionan un problema con una transacción).

2. Luego le dicen que debe ponerse en contacto con ellos, para lo que le indican un link, dentro del mail, que parece ser de un sitio legal, pero que en realidad es un sitio falso para estafar. La persona cree estar, por ejemplo, dentro del sitio de eBay, porque es idéntico, pero en realidad está en el sitio de los estafadores.

3. La persona se conecta al sitio e ingresa sus datos personales y financieros. Esa información queda copiada en una base de datos de los estafadores.

4. Con esa información a disposición, los estafadores pueden vaciarle la cuenta, generarle gastos en la tarjeta de crédito o hacerse pasar por esa persona.

Para protegerse del phishing se debe hacer lo siguiente:

1. Nunca haga clic en ningún vínculo dentro del mail que le enviaron. Si piensa que el mensaje puede ser de verdad, abra una nueva ventana en el navegador, tipee la dirección web del sitio (por ejemplo, www.ebay.com) y luego ingrese a su cuenta. Si se trata de su cuenta bancaria y tiene la posibilidad de consultar por teléfono, mejor aún.

2. Nunca entregue información personal y mucho menos números de tarjeta de crédito o bancarias y por supuesto nunca dé contraseñas.

3. Si le ocurrió que fue engañado y le entregó datos a los estafadores, comuníquese inmediatamente con su banco y con la empresa emisora de su tarjeta y avise lo que le pasó. Va a tener que bloquear sus cuentas y tarjetas para evitar perdidas económicas.