Mercado de Dinero
Fecha: viernes, 27 de febrero de 2015
Página: 11
Nº documentos: 1

Recorte en color % de ocupación: 5,26 Valor: 236,55€ Periodicidad: Mensual Tirada: 40.895 Difusión: 36.737

SEGURIDAD

Primer estudio europeo sobre el uso de 'cookies'

La Agencia Española de Protección de Datos ha participado en el primer análisis coordinado con otras autoridades europeas para examinar el uso de 'cookies' en algunas de las páginas web más visitadas. El análisis –en el que la AEPD ha participado junto a sus homólogos de Dinamarca, Eslovenia, Francia, Grecia, Países Bajos, Reino Unido y República Checa– ha examinado 478 sitios web, de tres sectores: comercio electrónico, medios de comunicación y servicios públicos.
Las conclusiones revelan que los responsables de los sitios web han tomado medidas para informar a sus usuarios sobre la instalación de 'cookies' en los dispositivos de sus visitantes, pero que aún deben mejorar en la obtención del consentimiento necesario para su uso.

HERENCIA VIRTUAL

Facebook activa un formulario para notificar la muerte

Facebook ha anunciado la posibilidad de designar un heredero virtual de la cuenta en la red social en caso de fallecimiento.
La comunicación del deceso a la red social se hará por medio de un formulario, que Facebook ha activado para que un amigo o familiar del usuario fallecido notifique a la compañía lo ocurrido. El formulario solicita el nombre y la fecha en la que ha fallecido, y, si es posible, también conviene adjuntar algún archivo, obituario o similar, que sirva como prueba. Con los datos enviados, Facebook comprueba la veracidad del fallecimiento.
La cuenta, entonces, pasa a ser conmemorativa, lo que significa que junto al nombre del usuario aparecerá escrito 'En Memoria', y amigos y familiares podrán compartir recuerdos sobre esa persona.

'BULLYING'

Un videojuego español contra el acoso escolar

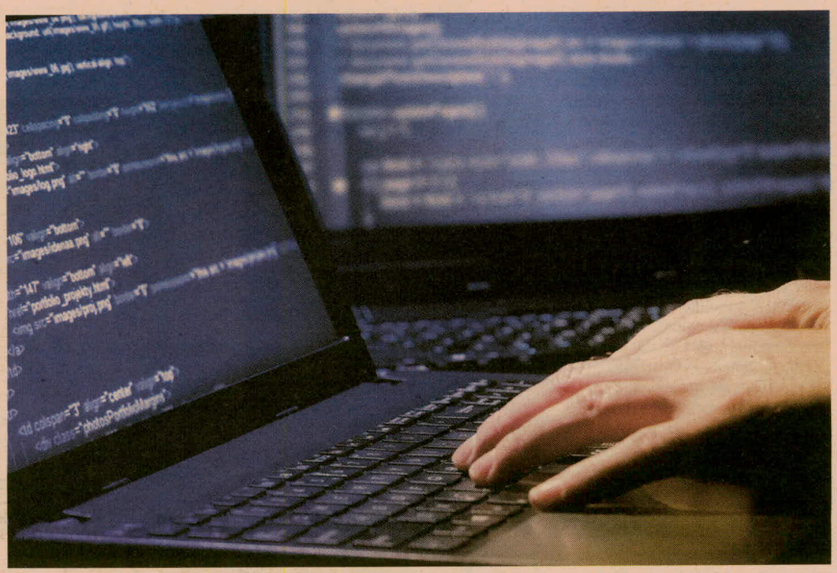
La empresa española Nesplora, con el aval del Ministerio de Industria, Energía y Turismo, ha desarrollado 'Monité', un programa integral en español para la prevención de conductas relacionadas con el acoso escolar o 'bullying'. El programa consta de cuatro ejes: un videojuego, disponible a través de Internet; manuales para padres con materiales específicos para trabajar con sus hijos, educadores y terapeutas; material complementario como vídeos y cuentos; y una página web para compartir experiencias y reforzar el aprendizaje.
Está dirigido a niños de entre 6 y 11 años y estará disponible desde el 16 de febrero en prereserva en la web www.monite.org.

El robo de identidad, un delito en auge en todo el mundo

Necesitamos leyes más fuertes para combatir el robo de datos

Por Eric T. Schneiderman
Fiscal General de Nueva York

El pasado mes de febrero se conocía la noticia de que un grupo de 'hackers' habían llevado a cabo una operación de 'limpieza' de las cuentas de más de un centenar de bancos de alrededor de 30 países. Una noticia que ponía en primer plano –si es que no lo estaba ya–, el debate sobre la seguridad informática. El robo de identidad es uno de los delitos de más rápido crecimiento en los Estados Unidos, donde llevan ya unos años articulando medidas para protegerse. En España, las cifras se han disparado: somos el país de la UE que más robos de identidad por Internet sufre, muy por encima de la media, según datos de Eurostat. Las denuncias ante la Agencia Española de Protección de Datos se han multiplicado por tres en un año. Conviene aprender cómo se está combatiendo en EE UU, para saber el camino que nos queda por recorrer. El fiscal general de Nueva York, Eric T. Schneiderman, dedica su artículo en este número de Mercado de Dinero a ello.



Las denuncias por robo de identidad por Internet ante la AEPD se han multiplicado por tres en apenas un año.

Pregunta: ¿qué tienen en común Target, Home Depot, Sony Pictures, JPMorgan Chase y el Servicio Postal de Estados Unidos? Si pensó que todos han sido víctimas de enormes violaciones a sus bases de datos, es posible que usted sea una de las decenas de millones de estadounidenses que se ha ocupado de cambiar sus contraseñas y revisar sus estados de cuentas de tarjetas de crédito para detectar cargos fraudulentos.
Las violaciones de datos ponen a individuos, empresas y agencias gubernamentales en riesgo, y están en aumento. El año pasado, mi oficina arrojó algo de luz con un informe en el que por primera vez se analizó ocho años de violación de la seguridad bases de datos para entender a quién afecta, cómo ha crecido el problema, y cuánto nos está costando.
Los números no son atractivos. Las brechas de seguridad de datos denunciadas en Nueva York se multiplicaron por más de tres entre 2006 y 2013. En ese mismo periodo, 22,8 millones de registros personales de los neoyorquinos quedaron expuestos en casi 5.000 violaciones de datos. Esas brechas de seguridad costaron a los sectores público y privado en nuestro estado más de 1.370 millones de euros en 2013. Además, el informe concluyó que la piratería e intrusiones –en la que terceros obtienen acceso no autorizado a los datos almacenados en un sistema informático– fueron la principal causa de las violaciones de seguridad de los datos, lo que representa aproximadamente el 40% de todas las infracciones.
Desafortunadamente, mientras que el riesgo crece día a día, la ley de Nueva York para proteger los datos personales no se ha actualizado desde que Facebook cumplió un año de haber sido puesto en marcha y 'tuitear' seguía limitado a las aves.

Entre 2006 y 2013, 22,8 millones de datos quedaron expuestos en NY

Es hora de actualizar la ley de seguridad de datos de Nueva York para ampliar y fortalecer la protección de los consumidores y recompensar a las empresas que toman medidas responsables para proteger los datos confidenciales de sus clientes.
Si bien una ley estatal no será una cura total, nuestro estatuto actual es obsoleto, sin fuerza y no se ocupa de algunos de los aspectos fundamentales del uso moderno de Internet. Tampoco logra crear una verdadera alianza entre las empresas y el Gobierno para elevar los estándares de seguridad, y la captura de los piratas.
Por ejemplo, la ley actual ofrece a las empresas una orientación insuficiente sobre qué datos deben ser tratados como privados y cómo proporcionar 'seguridad razonable de datos'. La ley exige que una empresa dé aviso a los consumidores y a la Oficina del Fiscal General sólo si hay una violación de "información privada", que se define como un nombre en combinación con un número de seguro social, permiso de conducir o un número de cuenta o tarjeta de crédito.
Podemos y debemos hacerlo mejor. Propongo un enfoque de tres vertientes:

- En primer lugar, ampliar las protecciones existentes.

La definición de "información privada" debe actualizarse para incluir la combinación de una dirección de correo electrónico y contraseña, así como una dirección de correo electrónico en combinación con una pregunta y respuesta de seguridad. También debe incluir información médica, información sobre el seguro de salud, y de forma crítica, los identificadores biométricos como las huellas dactilares, un tipo de datos que las empresas están almacenando cada vez con mayor frecuencia.

- En segundo lugar, debemos fortalecer la protección de información privada.

La ley actual no especifica una norma razonable y específica para la seguridad de datos, salvo si una entidad recoge los números de la Seguridad Social. Nuestra ley debería exigir medidas de seguridad técnicas, administrativas y físicas.

- En tercer lugar, hay que premiar a las empresas que van más allá de los requisitos mínimos legales para proteger a sus clientes.

Es importante recordar que las empresas son víctimas también, y si han tomado medidas responsables para proteger a sus clientes, no deben ser tratadas como culpables. Aquellas entidades que adoptan prácticas modélicas de seguridad de datos deben obtener protección parcial o total contra las demandas, o quizás exenciones fiscales.
Las empresas que comparten información sobre un incumplimiento con la ley a los efectos de atrapar al malhechor no deben perder el privilegio abogado-cliente o de protección de secretos de la información que divulgan. Esto animará a las empresas a cooperar con la policía en estos casos.
El riesgo de robo de datos afecta a todos los negocios y a cada familia. La nueva ley que propongo será la más fuerte y más completa de la nación. Actuemos ahora para hacer de nuestro Estado un modelo nacional para la privacidad y seguridad de datos.
Es hora de actualizar la Ley de Seguridad de Datos de Nueva York para ampliar y fortalecer la protección de los consumidores y recompensar empresas que toman medidas responsables para proteger los datos confidenciales de sus clientes.
Si bien una ley estatal no será una cura total, nuestro estatuto actual es obsoleto, sin fuerza y no se ocupa de algunos de los aspectos fundamentales del uso moderno de Internet.

Hay que premiar a las empresas que protegen a sus clientes