

INFORME CIBERSEGURIDAD



SEGURIDAD BANCARIA.

¿Están nuestros datos financieros realmente seguros en la Red?



Los bancos son parte de las llamadas “infraestructuras críticas” de un país. Esto significa que son instituciones clave para que una nación funcione con normalidad, al igual que el suministro eléctrico, el agua potable y un largo etcétera. Según datos del Instituto Nacional de Ciberseguridad (**INCIBE**), sólo en los seis primeros meses del año se han registrado 52 ciberataques a infraestructuras críticas.

España es el segundo que más ataques bancarios recibe. Las entidades financieras constituyen un sector crítico para la seguridad nacional, y global. Unos días sin la posibilidad de retirar dinero de los cajeros, o sin poder realizar pagos con tarjetas de crédito, puede provocar el caos en un país, y afectar de forma muy crítica a la estabilidad global.

Aunque es muy difícil atacar a un banco con éxito, no es la primera vez que esto sucede. Es el caso del

SEGURIDAD BANCARIA.

distribuidor estadounidense, Target que reconoció en 2013 haber sufrido un ataque de unos hackers que piratearon más de 40 millones de tarjetas de crédito y que supuso para los bancos EEUU pérdidas de más de 200 millones de dólares.

Otro caso más reciente fue el ataque en 2014 a JP Morgan Chase. Una invasión masiva y organizada de hackers burlaron la seguridad y accedieron a los datos de 76 millones de familias y 7 millones de empresas. Y aunque la empresa aseguró que sólo accedieron a los datos de contacto de los clientes, el incidente afectó a todos los usuarios de su portal o de su aplicación móvil.

Lo cierto es que el coste total de estos ataques es difícil de concretar porque muchos bancos no reconocen este tipo de delitos, no cabe duda de que junto a las cuantiosas pérdidas económicas que supone, hay otros costes, a veces, intangibles pero no menos elevados. De hecho, **un 47% de los encuestados para este informe declaran haber sufrido alguna estafa online.**

Phishing, fraudes a través de sms, compra-venta entre particulares, virus... Son sólo algunas de las artimañas a las que se enfrenta el usuario.

Según un informe de Fico de este año, a nivel europeo, el fraude más común es el que afecta a transacciones en las que no es necesario mostrar físicamente la tarjeta, es decir los pagos online. Este tipo de fraude supuso el 70% de los casos en 2014, frente al 10% de 2006, con especial incidencia en los pagos realizados a compañías de un país con tarjetas procedentes de otro.

Francia encabeza la lista de países con más fraude, seguido de Grecia y Reino Unido, este último con una elevada tasa de engaños basados en transacciones sin tarjeta (70%). España, sin embargo, se aleja de estos patrones. La falsificación (65%) y el robo o pérdida de tarjetas (22%) son las principales causas de pérdidas para los bancos.

DATOS PERSONALES.

¿Somos conscientes de la importancia de asegurar nuestros datos personales?



A la hora de movernos por Internet es muy habitual encontrarnos con registros obligatorios para tener acceso a servicios, información, descargas, etc. De hecho, la razón de ser de muchos sitios web aparentemente inofensivos es recolectar datos de usuarios registrados que luego puedan ser utilizados y monetizados de las más variadas maneras.

En España los datos personales están protegidos por la Ley, aunque hablamos de Internet, un territorio virtual en el que es relativamente fácil saltarse las normas sin consecuencias con solo, por ejemplo, ubicar los servidores en determinados territorios carentes de legislación.

El pasado mes de junio, Bruselas aprobó la nueva norma de protección datos que reconoce el “derecho al olvido”. Una norma que se ha debatido durante tres años con el fin de reforzar la protección de datos. Se aplicará a Facebook o Google y prevé fuertes multas por incumplimiento. Además, se procesará información personal con el “consentimiento inequívoco” de los usuarios.

La nueva normativa tiene por objeto adaptar las reglas vigentes en la UE sobre protección de datos, que databan de 1995, a la nueva realidad de internet

DATOS PERSONALES.

y las redes sociales, garantizar un mayor control de los usuarios del tratamiento de sus datos personales en la red y reducir las cargas burocráticas para las empresas por un valor de unos 2.300 millones de euros anuales. Los usuarios que se sientan perjudicados por el tratamiento de sus datos en internet tendrán derecho a reclamar sanciones que **podrán traducirse en multas de hasta un 2% de la facturación anual** o de un máximo de un millón de euros para la empresa que haya infringido el reglamento europeo. Estarán sujetas a estas normas todas las empresas que operen en territorio comunitario con independencia de dónde tengan su sede.

La Agencia Española de Protección de Datos avisa que en Internet, como en el mundo físico, nuestra actividad deja un rastro. Además de los datos personales que aportamos voluntariamente al darnos de alta en servicios como redes sociales, portales de contactos o de compra on-line, y de los datos personales propios que otros pueden publicar en sitios web sin nuestro conocimiento, nuestra navegación en Internet deja rastros que pueden identificarnos.

En el sitio web de la AEPD se pone a disposición de los

ciudadanos información, consejos así como recursos y materiales para fomentar una participación segura en las múltiples posibilidades que hoy nos ofrece Internet.

A la hora de facilitar datos de carácter personal en la Red hay que asegurarse de la fiabilidad y seguridad que nos ofrece quien los solicita, debiendo aportar, en todo caso, exclusivamente los necesarios para la finalidad con la que están siendo recabados. Para ello, debemos acudir a las políticas de privacidad y las condiciones de uso que se publican en los distintos sitios web.

A través de sitios web como redes sociales, portales de contactos, portales de video, blogs y foros se pueden “filtrar” datos personales en la Red sin conocimiento ni consentimiento del titular de los datos y, en muchas ocasiones, su indexación por los buscadores puede darles una difusión global en Internet. En la mayoría de los casos, y salvo excepciones, tenemos derecho a solicitar que se cancelen los datos publicados en esos sitios web o, al menos, a que se evite su recuperación por los buscadores. Para ello, debemos dirigirnos al responsable del sitio web que aloja el contenido con nuestros datos o también, en

el caso de los blogs y foros, al autor del contenido. Por otro lado, **las direcciones IP** también puede utilizarse para localizar geográficamente al usuario y, dado que se asigna unívocamente a la línea de conexión por la compañía que nos presta el servicio de acceso, puede permitir en muchos casos la identificación del titular de la línea y, en consecuencia, del probable usuario. Muchos servicios de Internet, como las redes sociales o los buscadores, conservan las direcciones IP de los ordenadores de sus usuarios.

En cuanto a **las cookies**, son ficheros que se almacenan en el ordenador del usuario que navega a través de Internet y que, en particular, contienen información sobre el sistema operativo y el navegador utilizados en la navegación. Estos ficheros se asocian a un número que permite identificar unívocamente el ordenador usuario.

Las cookies son creadas por el sitio web que visita el usuario y permiten a éste conocer con detalle su actividad en el mismo sitio o en otros con los que se relaciona éste, por ejemplo: el lugar desde el que accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo y navegador utilizados, las páginas más visitadas, el número de clicks realizados e infinidad de datos respecto al comportamiento del usuario en Internet.

Son importantes porque pueden permitir elaborar perfiles sobre nuestra navegación por Internet, los cuales se utilizan para analizar nuestros gustos y preferencias, con objeto de determinar nuestra idoneidad como participantes en campañas publicitarias, de marketing u otras actividades. Además, los efectos sobre la privacidad pueden tener un alcance mayor al que cabe pensar en un primer momento, ante la posibilidad de relacio-

nar su contenido con la dirección IP de conexión y con otros datos de carácter personal, como son los aportados por los propios usuarios al registrarse o los que pueden ser recopilados a través de modernas técnicas de minería de datos.

Los sitios web deben informarnos de la utilización de cookies. Además, es posible y recomendable, a través de las herramientas que proporciona el navegador que utilizamos, borrar regularmente las cookies que se almacenan en nuestro ordenador. Asimismo, deben ofrecernos la posibilidad de decidir sobre el uso de las cookies para realizar perfiles sobre nuestra navegación.

Según el estudio que ha realizado S2 Grupo, **el 22% de los encuestados reconoce dar sus datos personales si se los pide una web, sin tomar ningún tipo de medida de seguridad y obviando el riesgo que eso supone**. La compañía, también advierte a los usuarios que tengan presente que salvo que empleen mecanismos de cifrado, **el correo electrónico** en Internet no es seguro. Los mensajes de correo y los foros de discusión pueden ser objeto de falsificación y suplantación de personalidad, lo que debe tenerse en cuenta siempre que se usen.

En definitiva, se recomienda a los usuarios que utilicen las últimas versiones de los programas informáticos dada la incorporación en estos de mayores medidas de seguridad. Igualmente, se recomienda utilizar los mecanismos de seguridad que tengan a su alcance (servidores Web seguros, criptografía, firma digital, firewall, etc.) para proteger la confidencialidad e integridad de sus datos en la medida en que le resulte necesario, dado que existen riesgos de suplantación de la personalidad o violación de la comunicación.



TELEFONÍA MÓVIL.

¿La telefonía móvil es una nueva fuente de riesgos para los usuarios?



La sociedad española es una de las más conectadas, según el informe Sociedad de la Información 2014, y esto se debe en gran medida a que somos uno de los países con más penetración de estos dispositivos, sólo superada por Singapur. Lo cual nos da una idea de la importancia de proteger un dispositivo que desde hace tiempo guarda nuestras cuentas bancarias, el acceso a redes sociales, emails profesionales, fotos personales y mucho más.

Sin embargo, según el estudio que ha realizado S2 Grupo, **el 60% de los encuestados reconoce que no proteger su smartphone con ningún tipo de contraseña. Es más, un 33% reconocen compartir “información sensible”** a través de aplicaciones o servicios, muchos de ellos asociados al móvil, sin la percepción del riesgo que supone. Y el riesgo no viene sólo por la posibilidad de que nos roben el móvil, sino también a la hora de protegerlo de virus o malware que puede dañarlo y robarnos nuestros datos personales.

Según un informe de Incibe sobre “Malware y dispositivos móviles”, **una de las razones por las que los creadores de malware han decidido ampliar su**

TELEFONÍA MÓVIL.

rango de acción a los dispositivos móviles, es la gran cantidad de información de valor almacenada en ellos.

Desde nombres de usuario y contraseñas, documentos privados, datos de formularios y un largo etcétera con los que se frotan las manos los hackers.

Pero, ¿cómo se puede infectar un móvil? Normalmente las fuentes de infección suelen ser cuatro: los juegos y aplicaciones que se ofrecen en la redes sociales, el correo electrónico infeccioso que se abre desde del dispositivo, las redes wifi “públicas” y desconocidas y las tiendas de aplicaciones.

Mención especial merece este último apartado. Cada tienda virtual sigue su propia política para controlar las aplicaciones que se aprueban, siendo algunas más restrictivas que otras. Esto quiere decir que las aplicaciones son sometidas a controles más o menos rigurosos para detectar malware o comportamientos sospechosos en ellas antes de que puedan ser descargadas por el público. Aun así, se han dado casos de aplicaciones maliciosas disponibles en estos markets, con un resultado de millones de datos personales robados.

Tenemos que empezar a ser conscientes de que el peligro no es que nos roben en dispositivo, lo valioso es lo que realmente guardamos en él. Por eso es fundamental proteger nuestro dispositivo con una contraseña de encendido y desbloqueo, no instalar software de repositorios no oficiales, evitar compartir datos personales en redes WIFI públicas, realizar periódicamente una copia de seguridad y en el caso de que se pueda, instalar un sistema antimalware.

PERCEPCIÓN.

¿Qué medidas de ciberseguridad están presentes en tu día a día?



Como se dice normalmente no hay mejor remedio que la prevención. Ser conscientes de los peligros y amenazas de la seguridad de la información es en gran parte la solución para evitar ser víctimas de ciber delincuentes.

Las labores de concienciación que se desarrollan desde S2 Grupo son una de las herramientas más potentes que podemos encontrar en entorno Español. Conceptos como “Ingeniería Social” son los que nos permiten descubrir que no hay un mejor antivirus que ser previsores y hacer un uso responsable de nuestra información en medios digitales.

Según el decálogo de concienciación publicado por el INCIBE el nuevo escenario laboral, ha convertido a nuestro puesto de trabajo en móvil, pudiendo trabajar desde cualquier parte del mundo. Esto ha convertido a cada empleado en el nuevo perímetro de seguridad a proteger. Ante esta situación, la formación y la concienciación en ciberseguridad se convierten en iniciativas básicas y fundamentales.

Siguiendo el decálogo los tres pilares son: las perso-

PERCEPCIÓN.

nas, los procesos y la tecnología. El objetivo de la concienciación es trasladar las mejores prácticas en materia de seguridad. Los puntos más importantes son:

El puesto de trabajo

- Mantener la mesa “limpia” de papeles que con tengan información sensible
- Bloquear la sesión del equipo cuando se abandona el puesto de trabajo

Dispositivos

- No modificar la configuración de los dispositivos
- No instalar aplicaciones no autorizadas
- No conectar dispositivos USB no confiables
- Establecer una clave de acceso y la opción de bloqueo automático en dispositivos móviles

Equipos no corporativos

- No manejar información corporativa en equipos públicos
- No descargar ficheros si se accede si se accede

al correo corporativo desde un equipo personal

Fugas de información

- No facilitar información sensible si no se está seguro de quién es el receptor
- Destruir la información sensible en formato papel
- Mantener conversaciones confidenciales lejos de terceros

Gestión de credenciales

- No compartir credenciales de acceso
- No utilizar credenciales corporativas en aplicaciones personales
- No apuntar las credenciales en lugares visibles

Navegación

- Evitar acceder a páginas web no confiables
- No pinchar en enlaces sospechosos

PERCEPCIÓN.

Correo electrónico

- Eliminar todo correo sospechoso que se reciba
- Evitar los correos en cadena

Protección de la información

- Realizar copias de seguridad de la información sensible

Viaje seguro

- No transportar información sensible en dispositivos extraíbles
- No manejar información sensible en redes WIFI no confiables

Ser seguro

- Avisar al departamento de ciberseguridad si se detecta actividad sospechosa o un funcionamiento anómalo.

En relación a nuestra encuesta realizada a los usuarios de Hijos Digitales, 85 de 395 encuestados dicen dar

su información con facilidad en caso que un sitio web así se lo solicite. Esto demuestra que el 22% no tiene problema o demuestra preocupación sobre el uso de sus datos personales. Dentro del marco de la misma encuesta para el día internacional de la ciberseguridad, solo la mitad de los usuarios cierra la sesión luego de utilizar las redes sociales y el 60% no cambia sus contraseñas regularmente.

El liderazgo de S2 Grupo en el desarrollo de grandes proyectos de concienciación en ciberseguridad se fundamenta en sus programas **Protectit y Protegits** y en la compartición de información en sus blogs:

- **Security ArtWork**
- **Hijos Digitales**

ProtegiTs fue, inicialmente, un proyecto del ámbito de la Comunidad Valenciana que, liderado por la Dirección General de Modernización, dependiente de la Consellería de Justicia y Administraciones Públicas de la Generalitat, y junto con empresas valencianas de relevancia pretende incrementar la seguridad de los menores.

PERCEPCIÓN.

Actualmente forma parte del programa de responsabilidad corporativa de S2 Grupo para formar a los jóvenes en el uso seguro de la tecnología.

A diferencia de otras iniciativas en este campo, limitadas a un enfoque principalmente pasivo, ProtegiTs abarca tres áreas de acción bien diferenciadas:

- **Clases formativas:** dirigidas tanto a menores como a padres. El propósito de esta iniciativa es dar una visión real de las amenazas a los menores, con un contenido adaptado a los diferentes grupos de edad diseñados en el proyecto.
- **El Kit ProtegiTs:** formado actualmente por un complemento para navegadores y una aplicación, tiene la función de prevenir, detectar y facilitar la respuesta frente a potenciales amenazas a las que el menor pueda verse expuesto en su utilización de Internet.
- **El Blog hijos digitales:** un medio a través del cual, además de divulgar el proyecto, se ofrece información relevante, descargas de aplicaciones y recursos tanto para menores como para padres y docentes.

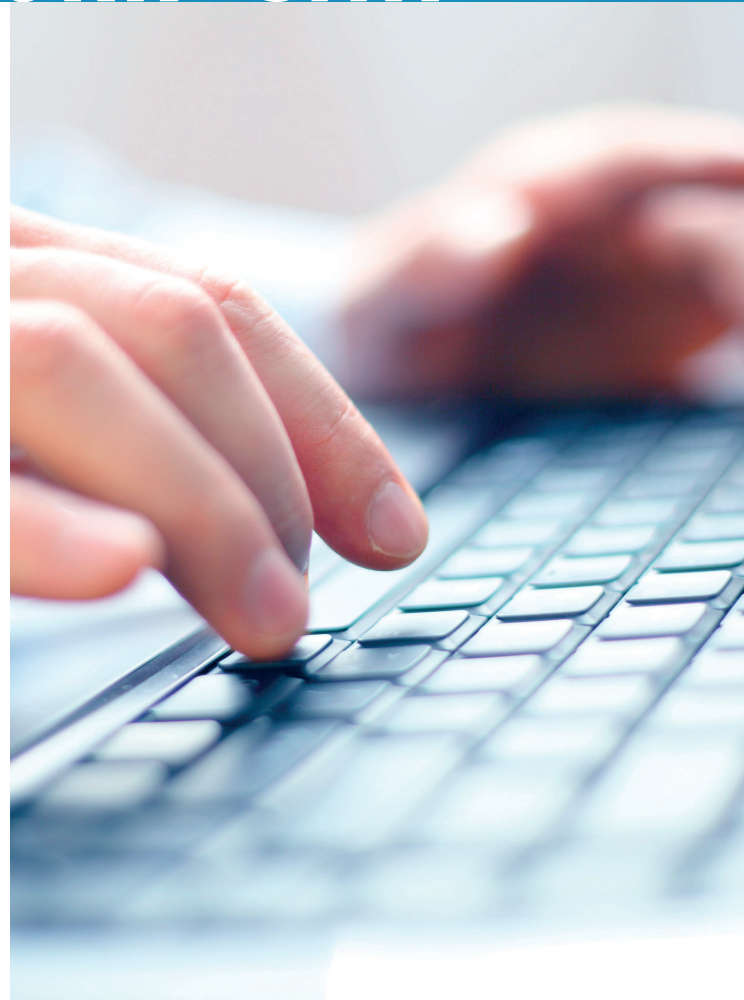


SECURITY ART WORK - SAW

Con mas de 20.000 visitantes únicos por mes, **SAW** es el blog de divulgación sobre los temas de la Seguridad de la Información en castellano más leído pro los profesionales del sector.

Se centra en todas las facetas de la seguridad, tanto desde el punto de vista lógico, como legal y organizativo (la física se limita a diseño de CPDs).

El tipo de contenidos va orientado a profesionales o personas interesadas en las nuevas noticias y novedades en materia de ciberseguridad.



HIJOS DIGITALES (BLOG)

El blog estrella de S2 Grupo, con más de 240.000 usuarios mensuales y hasta 12.000 usuarios por día. Todos los nativos digitales son “hijosdigitales”. Por tanto todos los que tienen hijos digitales bajo su tutela, conviven con “nativos digitales”. Esto en sí mismo no es ni bueno ni malo. Simplemente hay que tenerlo en consideración y tener muy claro que somos “inmigrantes digitales” incluso a pesar de que desarrollemos nuestra actividad profesional en este sector. Este es un hecho que no podemos cambiar. No se cambia con formación ni con información, simplemente es un hecho con el que tenemos que aprender a convivir.

Este es el objetivo del blog **Hijosdigitales.es** pretende ser un espacio de convivencia de dos generaciones: la de los “nativos digitales” y la de los “inmigrantes digitales”. Un espacio que nos sirva para que todos los actores que intervienen en este nuevo paradigma puedan conversar, intercambiar opiniones, resolver dudas, etc. En definitiva, hijosdigitales busca ser un punto de encuentro de tod@s los que estamos interesados en el uso seguro de los avances tecnoló-

gicos tanto por parte de nuestros jóvenes como por nuestra parte.

Detrás de hijosdigitales trabajan un grupo de profesionales especializados en seguridad, redes sociales, etc., en general, profesionales de la tecnología que preocupados por el uso que algunos colectivos desprotegidos hacen de estas herramientas.

Sin embargo, hijosdigitales no es sólo ni principalmente quienes lo crean. Detrás de hijosdigitales hay niñas y niños, jóvenes, padres y madres y por qué no abuelos preocupados por la seguridad en la red de sus nietos; han invitado a todos ellos, y a miembros de las fuerzas y cuerpos de seguridad del estado para que les ayuden en la medida de sus posibilidades a disipar algunas dudas que se puedan tener. Hijosdigitales es un blog y por tanto un espacio abierto, aunque moderado, en el que se busca la participación activa de distintos actores.



Anticipando un mundo
ciberseguro



Madrid
T (34) 902 882 992
Velázquez 150, 2ª planta
28002 Madrid



Barcelona
T (34) 933 030 060
Llull, 321
08019 Barcelona



Valencia
T (34) 963 110 300
F (34) 963 106 086
Ramiro de Maeztu, 7
46022 Valencia



Bogotá
T (571) 745 74 39
Carrera 11, N°93A-53,
Oficina 401



México
T (52) 55 2128 0681
Praga 44-7, México D.F.
06600