RIESGOS Y SEGURIDAD EN EL CONSUMO DE SMARTPHONES

Alicia Agüero Ortiz
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

En los últimos años se ha producido un crecimiento exponencial en el consumo de smartphones, tanto es así que en la actualidad el 60,8% de los usuarios de telefonía móvil disponen de este tipo de terminal de última generación. La característica distintiva de estos terminales es la integración de un sistema operativo móvil avanzado que los asemeja a los ordenadores personales, ahora bien, esta semejanza se extiende a sus amenazas de seguridad. En este sentido, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) ha presentado un "estudio sobre seguridad en dispositivos móviles y smartphones"[1], del cual proceden los datos que aquí se citan.

1. Conectividad, nuevas funcionalidades y sus riesgos

Con la aparición de los smartphones se produce un aumento del grado de conectividad y de aprovechamiento de la web. Existen principalmente tres posibilidades de conexión. La primera de ellas es el *Sistema Bluetooth*, cuyo uso se halla prácticamente estandarizado, disponiendo de esta tecnología el 90,1% de los usuarios de telefonía móvil. El método de uso menos perjudicial es el seguido por la mayoría, a saber, activarlo únicamente cuando se vaya a utilizar (58,6%). Ahora bien, otra alternativa de uso seguro para quienes necesiten tener este sistema siempre disponible (por ejemplo, por utilizar dispositivos manos libres vía Bluetooth en el vehículo) es mantenerlo oculto al resto de terminales (6,5%). Por el contrario, tenerlo activado y visible al resto de usuarios (13,2%) permite la conexión de otros equipos, aumentando las posibilidades de que se produzca un ataque, como el envío de malware. La segunda posibilidad es la *Conexión a Internet a través de una Red de Datos*, utilizada por el 73,2% de los encuestados. Los mayores riesgos de esta modalidad refieren a la tarificación contratada con el operador telefónico, siendo aconsejable disponer de una tarifa plana de datos en la que, una vez consumidos los Megas contratados, disminuya la velocidad del servicio, pero en ningún caso comience una tarificación adicional. Finalmente, la conexión a través de *Wi-fi* es utilizada por el 69% de los encuestados.

[1] http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_moviles_1C2012

Asimismo, los teléfonos móviles incorporan actualmente nuevas funcionalidades. El universo de las aplicaciones ha evolucionado significativamente, generalizándose su descarga especialmente en usuarios de smartphones, el 71% de ellos acceden a su correo electrónico desde el terminal, y un 72,5% descargan aplicaciones. A este respecto, es de radical importancia efectuar las descargas desde fuentes de confianza o repositorios oficiales[2], de lo contrario el terminal quedaría expuesto a la descarga de aplicaciones maliciosas. Estos buenos hábitos son conocidos por los usuarios de estas aplicaciones, pues un 95,5% asegura realizar sus descargas exclusivamente desde repositorios oficiales. Mención específica requieren las aplicaciones de geolocalización que utilizan un tercio de los encuestados, pues obtienen la posición del usuario y conllevan el riesgo de desvelar a terceros su posición geográfica.

2. Incidentes de seguridad

La concurrencia de incidentes de seguridad ha disminuido sensiblemente respecto al año 2011. Los incidentes de seguridad más habituales son el extravío (12,4%), el robo (11%), la infección por virus o malware (1,6%) y el fraude con perjuicio económico (2%). Existen distintas situaciones que pueden concluir en un fraude económico, aunque un 84,5% de los encuestados asegura no haberlas sufrido. Las más habituales son la recepción de mensajes que incitan a la contratación de servicios (9,3%), la recepción de mensajes invitando a páginas web (7,2%), y la solicitud de claves de usuario o información personal (5,7%). Consumado el fraude, la cuantía defraudada es mayor entre los usuarios de smartphone (una media de 164,28 €) que entre los usuarios de teléfonos móviles convencionales (una media de 80,68 €).

3. Recomendaciones

Las novedades introducidas por los smartphones exigen la adopción de medidas de seguridad más intensas, similares a las aplicables a los ordenadores personales. Para evitar que los incidentes de seguridad puedan conllevar un fraude económico es recomendable conservar, además del PIN, el número de serie o IMEI (que podemos encontrar en la caja del terminal u obtenerlo pulsando la secuencia *#06#) con el cual el operador podrá bloquear el terminal. También es aconsejable bloquear el terminal tras su uso y configurar un mecanismo o contraseña de desbloqueo. En los smartphones, el usuario puede descargar aplicaciones gratuitas antirrobo y sistemas de localización[3], así como descargar antivirus gratuitos[4]. Además, existen programas que permiten generar

[2] *AppStore* de Apple, *Google Play* de Android o *App World* para Blackberry
[3] *Cerberus* para Android, *Buscar mi iPhone* para Apple, o *BlackBerry Protect* para BlackBerry
[4] *AVG Antivirus* para Android, *Lookout Mobile Security* para Android, BlackBerry y Windows Mobile, etc.

copias de seguridad mediante la conexión a internet o a un ordenador personal. Todo ello, debe ir acompañado de una actitud precavida del usuario quién debería descargar aplicaciones únicamente de repositorios legítimos y de fabricantes reconocidos.

En relación a la conectividad, hemos de activar la conexión Bluetooth cuando vayamos a utilizarla efectivamente, y en caso de necesitar su conectividad permanentemente, mantenerla oculta al resto de usuarios. Evitar realizar operaciones con datos privados (ej. transacciones económicas) a través de redes Wi-fi públicas. Y, por supuesto, proteger la privacidad, hacer copias de seguridad puntuales seguidas de borrados seguros de la información almacenada, comprobar los permisos otorgados a las aplicaciones descargadas, evitar almacenar fotografías e informaciones sensibles, en fin, todas las cautelas propias de la utilización de equipos informáticos pero con las especialidades relativas a su tamaño y fácil sustracción.