JULIO 2016

AUTOR: BORJA DÍAS

Nº 317

FICHA TÉCNICA

Título: **Estudio sobre la ciberseguridad y confianza en los hogares españoles**

Año: 2016

Fuente: ONTSI

Nº de páginas: 73

Acceso/coste: Gratuito

Localización: Disponible en el siguiente link

CONCLUSIÓN PRINCIPAL

La mayoría de los dispositivos están configurados de forma que permiten la instalación de aplicaciones desde fuentes desconocidas, con el riesgo que ello conlleva, además la mayoría de los reportes de incidencias tiene que ver con el famoso spam, afectando a mas del 87% de las víctimas, mientras que lo relacionado con virus afecta únicamente al 34,6%.

También hay que tener en cuenta únicamente un 25% de los usuarios han declarado haber tenido problemas de malware, mientras que el impacto real es muy superior al declarado, ya que se han declarado un 60% de ordenadores infectados por malware durante el periodo estudiado.

Además se observa que, sobretodo en dispositivos Android, el porcentaje de infecciones aumenta cuanto menos actualizado esté el dispositivo.

A pesar del gran número de usuarios con su red inalámbrica expuesta, únicamente un 14% sospecha haber sufrido algún tipo de intrusión en su red.

Los objetivos que el fraude persigue, es el de poder estafar con cifras lo suficientemente pequeñas para evitar que se considere delito penal, es decir, las estafas rondan sobre los 200€ siento la gran mayoría inferiores a los 100€.

AUTORÍA

El informe "Estudio sobre la Ciberseguridad y confianza en los hogares españoles" es elaborado por la ONTSI desde el 2014. Los datos de este informe abarcan el análisis desde Julio hasta Diciembre del 2015

En este estudio se valora sobre la conciencia de la gente ante el fraude al que se puedan enfrentar en la red, al igual de las diferentes formas que ay tanto de protegerse como de fraude. También se habla sobre los hábitos del comportamiento en la red y sobre las consecuencias de los incidentes de seguridad y reacción de los usuarios.

DESCRIPCIÓN Y CONTENIDO

El estudio se estructura en 8 bloques diferentes, en el primero de ellos nos hacen una breve introducción sobre los realizadores del informe y los objetivos que pretenden. En el segundo apartado primero definen y clasifican las medidas de seguridad, hablan del uso de estas medidas de seguridad, la frecuencia de la actualización y utilización, medidas de seguridad utilizadas en redes inalámbricas y uso de medidas en Android. El tercer párrafo nos introduce los hábitos de comportamiento en la navegación y uso de internet, tanto en banca en línea como en descargas de internet y hábitos de uso de Android y redes Wifi. En el cuarto capítulo introducen los incidentes en seguridad. En el quinto capítulo ya nos introducen las consecuencias de los incidentes en seguridad y como reaccionan los usuarios, como los cambios adoptados tras un incidente de seguridad. El sexto capítulo incluye la confianza en el ámbito digital en los hogares españoles. En el séptimo capítulo estarían las conclusiones finales y ya en el octavo la ficha técnica del estudio realizado.

ESTRUCTURA DEL INFORME

1. **Introducción al estudio**
2. **Medidas de seguridad**
3. **Hábitos de comportamiento en la navegación y usos de internet**
4. **Incidentes de seguridad**
5. **Consecuencia de los incidentes en seguridad**
6. **Confianza en el ámbito digital en los hogares españoles**
7. **Conclusiones**
8. **Alcance del estudio**

OTRAS CONCLUSIONES

De las principales medidas se seguridad automatizables se encuestas los software antivirus con un 75% y las actualizaciones del sistema operativo con un 57%. De las medidas no automatizables un poco mas del 50% de los usuarios dicen tener contraseña para proteger su equipo y documentos y un 47% borra los archivos temporales y cookies generados por el navegador.

En cuanto a lo que los usuarios revelan respecto a la realidad que nos revela Pinkerton, los que más diferencias muestran son el cortafuegos que los usuarios muestran un uso de un 41% frente al real que es de un 91%, por otro lado la utilización habitual con permisos reducidos son un 13 y 79% respectivamente.

Si hablamos de las redes inalámbricas Wifi, un 14% de los usuarios deja su red inalámbrica desprotegida o desconocen el estado en el que esta se encuentra. El 51% la protege mediante el sistema WPA o WPA2.

Las principales medidas de seguridad anunciadas por los usuarios de los dispositivos Android, son un 75% usan un sistema de bloque de pin o con patrón, un 70% tiene un software antivirus y un 65% configura el bloqueo automático después de un periodo de inactividad.

La mitad de los usuarios en redes sociales tiene su perfil configurado para que sea accesible solo por sus amigos o conocidos, mientras que un 31% expone que lo tiene publico y accesible para terceras personas desconocidas y un 6% no saben como tiene la configuración de su perfil.

En cuanto a la tipología de los malware detectados se aprecia que las infecciones de aldwares y troyanos es bastante más elevado en los PCs que en los dispositivos Android, sin embargo el malware espía es un 2% mas elevado en los dispositivos Android que en los PCs.

El intento de fraude en internet, un 34% de los usuarios destaca no haber sufrido ninguna situación de fraude frente al 66% que si dicen haber sufrido alguna situación de fraude.

Si hablamos de los cambios adoptados tras un incidente de seguridad, únicamente un 24% ha realizado un cambio después del incidente frente al 76% que no realiza ningún cambio. Dentro de los que realizan cambios, el principal es cambiar las contraseñas con un 32% y el segundo que mas es la actualización de las herramientas de seguridad ya instaladas con un 22%.

En cuanto al nivel de confianza en internet, un 44% confía bastante o mucho en internet frente a 1% de la población que desconfía de internet.