

PROYECTO FINAL DE INGENIERÍA INFORMÁTICA

Seguridad informática: Confidencialidad de datos



USAL
UNIVERSIDAD
DEL SALVADOR

Inés Rodríguez Piola

2014

INDICE

ABSTRACT	5
INTRODUCCION	6
PROBLEMATICAS ACTUALES SOBRE CONFIDENCIALIDAD DE DATOS	7
ANALISIS DEL ESTADO ACTUAL DE LA SEGURIDAD	19
1- Métodos más utilizados	19
Ingeniería social	19
Riesgos para las empresas	19
Forma de operar	20
Métodos más utilizados	21
Como educar a las personas	23
Phishing	25
Modalidad más utilizada	25
Phishing en los últimos diez años	26
Phishing en la actualidad	31
Aplicaciones Online	36
SQL Injection	37

Cross Site Scripting	38
Qué hacer	38
Mobile Malware	40
Categorías más atacadas	41
Ataques más comunes	42
Dispositivos rooteados	43
Permisos de las aplicaciones	44
Sistemas desactualizados	46
Java desactualizado	47
2- Delitos informáticos	50
Fraude	50
Robo	50
Robo de identidad	52
Skimming	54
Extorsión	57
3 - Precauciones	60
En las empresas	60



En los gobiernos	61
Protección de empresas frente a los gobiernos	62
Incrementa una nueva educación	66
Qué hacer como individuos	68
4 - Aspectos Legales	69
Constitución Nacional	69
Ley 26.388	69
Ley 25.326	70
Protección de datos personales	71
Habeas Data	71
5 - Conclusión	73
GLOSARIO	74
BIBLIOGRAFIA	77



ABSTRACT

Desarrollar cómo en la actualidad nuestros datos personales son vulnerables a ser obtenidos por terceros sin importar nuestro consentimiento. Cuáles son las amenazas más utilizadas contra los sistemas para obtener nuestros datos. Identificar los riesgos que corremos al perder el control de nuestros datos privados. Técnicas que se pueden utilizar para que un sistema sea seguro en este aspecto. Ver qué leyes hay al respecto para la protección del usuario. Analizar de qué manera podemos proteger nuestros datos.



USAL
UNIVERSIDAD
DEL SALVADOR

INTRODUCCION

En los últimos años debido a la evolución de la tecnología y a la constante interacción de los usuarios con internet crecieron las quejas y preocupaciones con respecto a la violación de la privacidad y al uso indebido de nuestros datos personales.

Esta nueva era donde interactuamos constantemente con la tecnología parece habernos simplificado la vida ayudándonos en ciertos casos, pero también estamos creando grandes bases de datos con información personal delicada que en caso de caer en manos no deseadas podría vulnerar nuestra intimidad.

El uso de redes sociales es prácticamente una necesidad hoy en día aunque no todos somos conscientes de la cantidad de información que ponemos a disposición de los demás. Lo mismo ocurre con los celulares, en los cuales almacenamos datos privados pero luego no prestamos atención a los permisos que se requieren a la hora de descargar e instalar aplicaciones. Éstos son sólo dos de los muchos casos que ponen en riesgo nuestra vida privada.

Entonces, el propósito de este proyecto es analizar el estado actual de la seguridad informática con respecto a la confidencialidad de nuestros datos y privacidad.

Para esto, se investigará si los motivos de las crecientes quejas son reales, o son solo preocupaciones por falta de conocimiento. También se analizará si las empresas toman los recaudos necesarios frente a estos problemas, o en caso contrario, ver qué leyes se ocupan de protegernos.

PROBLEMÁTICAS ACTUALES SOBRE CONFIDENCIALIDAD DE DATOS

Debido a que el objetivo de este proyecto es analizar el estado actual de la privacidad digital, se enumeran a continuación una serie de problemáticas con respecto a errores cometidos en los últimos años por grandes compañías de Internet, por los propios usuarios, y por los gobiernos, los cuales generaron polémica internacional.

Google admitió juntar datos privados por 'error' con Street View:

En el 2010 Google admitió que por más de tres años estuvo coleccionando de forma inadvertida información privada de las redes WiFi que no estaban protegidas.

Los hechos salieron a la luz porque las autoridades del Gobierno alemán pidieron a la compañía que les dejara auditar los datos que recopilan los autos con los que se cartografían las calles para hacer los mapas.

A raíz de estas preguntas, Google se dio cuenta de que los autos no sólo fotografiaban las calles, sino que también recogían información de las redes inalámbricas de los vecinos.

Días más tarde, Google confesó su error. Alan Eustace, el vicepresidente de Ingeniería e Investigación, escribió que un examen del software para Street View ha puesto de manifiesto que, debido a un error de programación en el año 2006, la empresa equivocadamente había estado recogiendo fragmentos de datos que eran transmitidos a través de redes WiFi sin contraseña alrededor de los cuales los autos de Google pasaban. Esto ocurrió en Europa, en los Estados Unidos y en otras ciudades importantes.

Eustace trató de restar importancia a la revelación, diciendo que Google "no utiliza esos datos en ninguno de los productos de Google." Él dijo que recogió sólo fragmentos de datos, ya que los coches se movían constantemente y cambiando canales muchas veces cada segundo. Sólo cuando alguien estaba usando su red sin contraseña y no encriptada los datos eran recogidos y almacenados.