INICIO GRABACIÓN

SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR

SEGURIDAD EN DISPOSITIVOS MÓVILES (SMARTPHONES, TABLETAS) Y EN REDES WIFI

OBJETIVOS

- CONOCER LAS PRINCIPALES AMENAZAS DERIVADAS DEL USO DE DISPOSITIVOS MÓVILES.
- CONOCER LOS DAÑOS QUE PUEDEN OCASIONAR A MI NEGOCIO LOS ATAQUES A MIS DISPOSITIVOS.
- PROTEGER MIS DISPOSITIVOS MÓVILES.
- TOMAR MEDIDAS DE SEGURIDAD PARA DISMINUIR LOS RIESGOS ASOCIADOS AL USO DE LOS MÓVILES, SUS APLICACIONES Y UTILIDADES.
- APRENDER ESTRATEGIAS PARA PROTEGER UNA RED WIFI.

INTRODUCCIÓN

- Los dispositivos móviles (smartphones, tabletas, etc.), se han convertido en una herramienta básica para cualquier trabajador con independencia de su profesión.
- Las funcionalidades que ofrecen son similares a las de los ordenadores pero también incluyen otras, como por ejemplo la geolocalización GPS o la cámara de fotos.

¿POR QUÉ PROTEGER LOS DISPOSITIVOS?

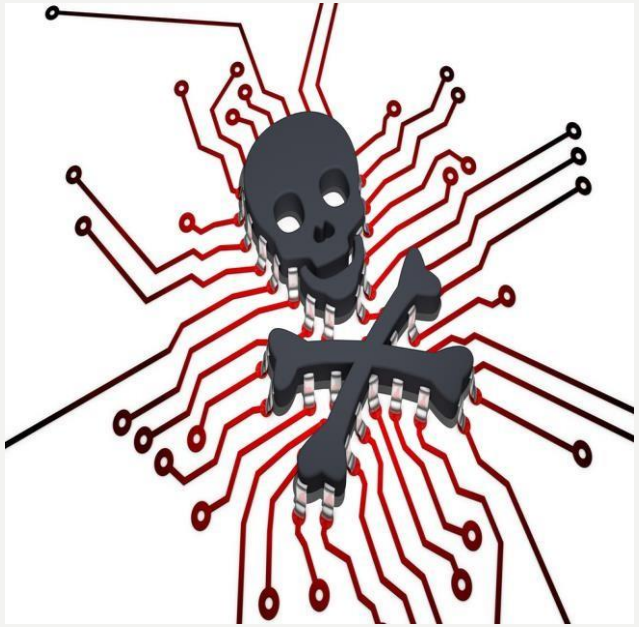
- Estos dispositivos no son precisamente baratos. Además su funcionalidad nos permite manejar una gran cantidad de información (cuentas de correo, documentos, nuestra agenda, contactos, fotos, credenciales de acceso…)
- Por estos motivos, los ataques a los dispositivos móviles son hoy en día frecuentes.Veamos los tipos en los que se pueden dividir.

¿POR QUÉ PROTEGER LOS DISPOSITIVOS?

ATAQUES IN-SITU

- La sustracción de dispositivos móviles es uno de los principales objetivos en hurtos y robos.
- El valor de algunos de estos dispositivos puede ser bastante elevado lo que los hace más apetecibles para ladrones y bandas organizadas.
- En este tipo de ataques, la información almacenada en el dispositivo no es el objetivo principal.
- Muchas compañías ofrecen seguros sobre los dispositivos, pero OJO , siempre que haya sido por robo, es decir con violencia (el hurto o la pérdida no suelen estar cubiertos).

CIBERATAQUES



Además tienen riesgos específicos asociados a las nuevas funcionalidades que incorporan, como los mecanismos de localización vía GPS o los protocolos de comunicaciones wifi, NFC y Bluetooth.

- Infección del dispositivo a través de malware.
- Ataques de *phishing* a través de mensajes o web.
- Aprovechamiento de vulnerabilidades de nuestro dispositivo.
- Acceso a un falso punto de acceso wifi (rogueAP) al que nos atrae un atacante para robarnos información.
- Abuso de permisos de aplicaciones

¿ EN QUÉ AFECTAN ESTOS ATAQUES?

Puedes experimentar:

- **Pérdida de confidencialidad** por robo de información contenida en el dispositivo o que se pueda acceder desde él, desde una fotografía personal hasta un documento confidencial almacenado en nuestra cuenta de Dropbox.
- **Pérdida de integridad** por modificación de los archivos o documentos almacenados en nuestro dispositivo, como una infección por malware, o cuando los cifran para pedirnos un rescate.
- **Pérdida de disponibilidad** si nuestro dispositivo no funciona correctamente o no es capaz de realizar ciertas tareas.

¿CUÁLES SON LAS INTENCIONES DE LOS ATACANTES?

- **Robo de información empresarial en beneficio suyo o de terceros**, causando daños económicos, pérdida de clientes,... como por ejemplo si nos roban nuestros «contactos de clientes».
- Robo de información personal y posterior **extorsión para recuperar los datos** amenazándonos con publicarlos. Ejemplos de este tipo son los robos de fotos íntimas o videos comprometedores.

¿CUÁLES SON LAS INTENCIONES DE LOS ATACANTES?

- *Tracking* (seguimiento) del propietario del dispositivo móvil a través de los datos de GPS, uso de wifi,… El objetivo es **obtener información de los lugares que frecuentamos, nuestras rutinas, etc.** Por ejemplo pueden controlar nuestra presencia o ausencia de nuestra tienda/empresa para robar en ella.
- **Utilizar nuestro dispositivo** para sus propios fines, convirtiendo nuestro dispositivo en «*zombie*» utilizándolo **para realizar ataques desde él,** como envío de spam,… Por ejemplo, si utilizan nuestro dispositivo, junto con otros, para saturar una página de un banco y no permitir a sus clientes utilizarla.

EJEMPLO

- Un empresario sufre un ataque a su dispositivo móvil y los atacantes toman el control del mismo. Estos, envían correos de spam desde las cuentas vinculadas al dispositivo que son las del correo corporativo.
- Al enviar SPAM desde nuestras cuentas de correo, nuestra dirección de correo así como el dominio de nuestra empresa han sido introducidas en listas negras. A partir de este momento, todo el tráfico saliente de la empresa es bloqueado por los filtros antispam de nuestros clientes y proveedores, y el negocio se ve seriamente perjudicado.

PROTECCIÓN DE ACCESO AL DISPOSITIVO

Patrón de Seguridad:

Camino realizado a través de una matriz de 3x3 o de una dimensión mayor. Debe pasar por al menos 4 puntos de la matriz (cuanto más largo sea más seguro será).

Es preferible que la aplicación no marque el camino configurado, y sea transparente, así dificultamos su aprendizaje a un mirón.

PROTECCIÓN DE ACCESO AL DISPOSITIVO

Huella dactilar:

Los dispositivos más modernos cuentan con un **lector de huella dactilar**, que permite que únicamente el dueño, que previamente ha guardado su huella, sea el que puede desbloquear el teléfono.

PROTECCIÓN DE ACCESO AL DISPOSITIVO

PIN:

Un **código**, normalmente de cuatro dígitos para restringir el acceso al dispositivo.

Evita códigos de seguridad vulnerables como 0000,1234 o fechas. Cuanto más aleatorio, más seguro será.

PROTECCIÓN DE ACCESO AL DISPOSITIVO

Imagen:

Se basa en el **reconocimiento facial** del dueño del terminal, el dispositivo es capaz de reconocer el rostro, y en función de eso desbloquear el terminal.

Este método no es recomendado debido a la facilidad de saltarse el control por parte de terceros, con una simple fotografía o video.

COMO DISMINUIR EL RIESGO

Ante una pérdida o robo hay que asegurarse de no perder los datos almacenados en el teléfono. **Podemos salvaguardar la información almacenada de dos formas:**

- **Copia de Seguridad**
- **Cifrado**

COPIAS DE SEGURIDAD

- Las copias se seguridad o backups, son **copias de respaldo de la información almacenada en el teléfono**, por ejemplo: lista de contactos, fotografías, información guardada de correos corporativos/personales, etc. Los backups nos garantizan **poder recuperar la información importante en caso de que surja un imprevisto**.
- Se puede realizar en local o en la nube. Permite sincronizar los contactos, el correo, el calendario o las fotografías de manera instantánea. Los sistemas de almacenamiento en la nube más conocidos en función del sistema operativo, son:
    - Android: Google Drive
    - iOS:Apple iCloud

CIFRADO

- La información que se almacena en los *smartphones* y tabletas se ha vuelto atractiva para los delincuentes que pueden llegar a ella tanto mediante acceso físico (robo, descuido, pérdida del dispositivo) como a través de aplicaciones maliciosas.
- Con el objetivo de proteger la información almacenada en los dispositivos, es muy recomendable **cifrarlos** aunque el rendimiento del teléfono se vea reducido.

CIFRADO

ANDROID

Permite cifrar el teléfono desde la versión Honeycomb (3.0) y hay diferentes tipos:

- **Cifrado de particiones de usuario**: desde la versión Honeycomb (3.0).
- **Cifrado completo:** a partir de la versión Lollipop (5.0). **Proceso**: ir a Ajustes > Seguridad > Cifrado con el móvil o tableta enchufados. El cifrado se realizará a través de una contraseña (es recomendable guardarla en lugar seguro). Es posible cifrar todo el dispositivo, incluyendo SD externa

IPHONE

Permite cifrar el teléfono desde la versión de iOS 4 a través del panel de Ajustes.

- **Cifrado normal**: a partir de iOS 4, los usuarios pueden decidir cifrar el teléfono asociándolo a una clave que sólo conozca el dueño. Sin conocer la clave no se podrá acceder al contenido del terminal.
- **Cifrado por defecto**: a partir de los modelos de iPhone 6 (iOS 8), su contenido está cifrado por defecto, asociado a la huella dactilar o a una clave

ACTUALIZACIÓN DEL SISTEMA Y DE LAS APLICACIONES

Las actualizaciones además de mejorar las capacidades del sistema y de las aplicaciones, **solucionan fallos de seguridad y vulnerabilidades** que, de no corregirse, pueden poner en peligro el dispositivo y la información almacenada en él.

ACTUALIZACIÓN DEL SISTEMA Y DE LAS APLICACIONES

Beneficios de aplicar actualizaciones:

- **Sistemas más seguros:**
- Resolución de vulnerabilidades
- Mejoras en la protección de la información
- **Nuevas funcionalidades:**
- Novedades en las funcionalidades del sistema
- Cambios en el diseño
- **Mejoras de rendimiento:**
- Sistemas que aprovechan mejor las capacidades del teléfono
- Menor consumo de batería

LOCALIZACIÓN EN CASO DE PERDIDA

Los *smartphones* cuentan con GPS, lo que pone al alcance de la mano servicios muy prácticos como:

- **Mapa** para indicarnos cómo llegar a un destino.
- **Guardar imágenes con datos de posición** de dónde está realizada la fotografía.
- **Tracking de deportes:** si se sale a correr, montar en bici… se pueden obtener datos de la ruta realizada, la intensidad del ejercicio, etc.
- **Juegos:** cada vez más juegos están relacionados con la ubicación, como por ejemplo búsquedas de tesoros.

Lookout Mobile Security:

Disponible para iP
Guarda la pos
el móvil
Tam

Prey

Disponible para iPhone y Android. Tiene la funcionalidad de hacer fotos a distancia con la que podremos «capturar» la imagen del ladrón.

Buscar mi iPhone

Como indica el nombre sólo es para productos de Apple (iPads y iPhones). Viene instalada por defecto. Permite localizar el dispositivo perdido si está activada la ubicación.

APLICACIONES PARA LOCALIZACIÓN

Administración de dispositivos:

Opción dentro de las opciones de seguridad en los teléfonos Android. Permite localizarlo, hacerlo sonar o borrar los datos, desde una página web.

CONEXIONES INALÁMBRICAS EN DISPOSITIVOS MÓVILES

Los dispositivos móviles incluyen una serie de tecnologías inalámbricas (wifi, Bluetooth, NFC) que proporcionan diferentes funcionalidades:

WIFI

Permite a los dispositivos conectarse a Internet de manera inalámbrica.

- Acceso a Internet
- Acceso a la red interna para compartir datos y sincronización

Bluetooth

Permite la transmisión de voz y datos entre diferentes dispositivos conectados entre sí mediante un enlace por radiofrecuencia.

- Transmisión de datos (fotografías, música, documentos...)
- Auriculares inalámbricos
- Teléfono manos libres y ordenadores de abordo en los coches

NFC

Tecnología de comunicación inalámbrica de corto alcance (unos 20 cm) y alta frecuencia que permite el intercambio de datos entre dispositivos. Usos:

- Identificación
- Recogida/Intercambio de datos
- Pago con el teléfono móvil

POSIBLES ATAQUES A TRAVÉS DE LAS CONEXIONES INALÁMBRICAS

WIFI

- **Man in the middle (MITM):** un usuario malintencionado se pone a «escuchar» entre el dispositivo e Internet y obtiene información de las acciones que realizamos con él y la información que enviamos (datos bancarios, redes sociales, información confidencial de la empresa...).
- **Robo de información pasivo:** pueden obtener datos de nuestra ubicación a través de las señales que el dispositivo envía para buscar redes wifi cuando no está conectado.

POSIBLES ATAQUES A TRAVÉS DE LAS CONEXIONES INALÁMBRICAS

Bluetooth

- **Bluejacking**: envían spam a la víctima mediante notas, contactos, imágenes, etc. Puede resultar peligroso y convertirse en una denegación de servicio dirigida a un objetivo o a un espacio (por ejemplo un bar).
- **Bluesnarfing**: aprovecha vulnerabilidades conocidas para obtener información del dispositivo atacado.
- **Bluebugging**: aprovecha bugs (fallos de programación) para ejecutar comandos en el terminal y controlarlo.

POSIBLES ATAQUES A TRAVÉS DE LAS CONEXIONES INALÁMBRICAS

NFC

- **Ejecución programas maliciosos:** ejecuta código en terminales Android simplemente acercando una etiqueta NFC al dispositivo.
- **Pagos sin autorización:** realiza compras por proximidad sin consentimiento
- **Transmisión de datos sin cifrar:** lee datos como el nombre, apellidos, el número de la tarjeta y en algunos casos las transacciones realizadas.

ALMACENAMIENTO DE INFORMACIÓN EN LA NUBE

todos los dispositivos se pueden conectar a la nube.

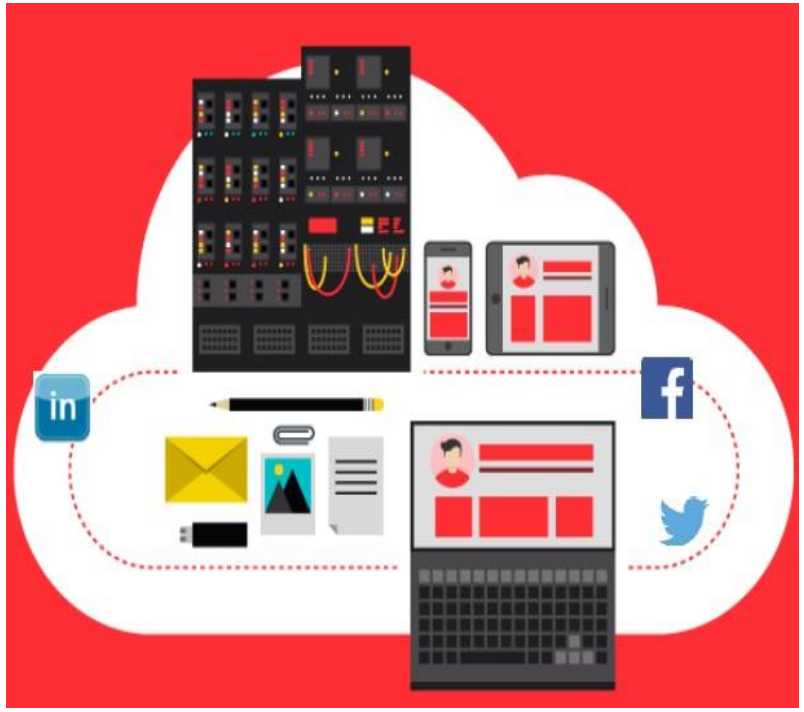
- Hay aplicaciones que guardan la información en la nube aunque aparentemente nos parezca que se almacena en el dispositivo, por lo que **es importante que seamos conscientes de dónde se almacena nuestra información para saber si está expuesta y cómo protegerla.**

Ejemplos

- Evernote 
- Google Drive 
- Dropbox 

ALMACENAMIENTO DE INFORMACIÓN EN LA NUBE

- En la actualidad se puede ***sincronizar el contenido de los dispositivos móviles** (información y aplicaciones) **con cuentas personales** para mantenerlo todo centralizado y poder **acceder a la información desde distintos dispositivos.**



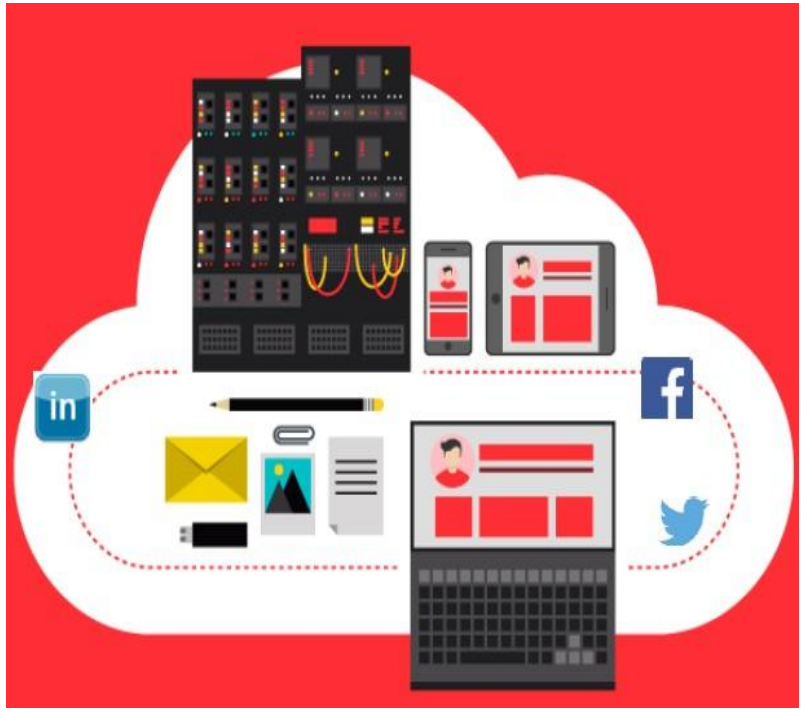
=

Peligros

- **Información confidencial en la red:** cada vez hay más información personal y de más valor en la red.
- **Servicios conectados entre sí:** que permiten iniciar sesión con el login de terceros, por tanto **la misma llave abre cada vez más puertas.**

ALMACENAMIENTO DE INFORMACIÓN EN LA NUBE

- En la actualidad se puede ***sincronizar el contenido de los dispositivos móviles** (información y aplicaciones) **con cuentas personales** para mantenerlo todo centralizado y poder **acceder a la información desde distintos dispositivos.**



=

Peligros

Social Login o conectores sociales

Autentificación con nuestras cuentas de Facebook, twitter, LinkedIn,... en otros servicios (Skype, Pinterest, Flipboard,...)

AUTENTICACIÓN MULTIFACTOR

Para proteger la información tanto al acceder a los dispositivos como al acceder a un servicio o a las aplicaciones se utilizan mecanismos para:

- **Identificarnos** o decir quienes somos, por ejemplo mediante nuestro nombre de usuario.
- **Autenticarnos** o mostrar que en realidad somos nosotros, para ello utilizamos uno o varios de estos **factores**:
  - **Algo que sé: sólo lo conoce la persona que quiere autenticarse**, como una contraseña o un PIN.
  - **Algo que tengo:** algún **objeto en posesión de la persona que quiere autenticarse**, como la SIM de un móvil, los *tokens* o dispositivos que generan contraseñas, o las tarjetas de coordenadas.
  - **Algo que soy:** referido a la biometría, **algo que puede ser medido y único de cada persona**, como la huella dactilar o el iris del ojo.

Las aplicaciones que utilizan mecanismos de autenticación que solicitan dos o más factores son más seguros que los que sólo utilizan uno.

SEGURIDAD AVANZADA

- Las **aplicaciones** móviles aprovechan la funcionalidad de los dispositivos para ofrecernos todo tipo de utilidades: juegos, redes sociales, envío de correos, información sobre el tiempo, horarios de transporte o noticias, entre otras.
- Las aplicaciones **se descargan** desde los **markets oficiales** de los teléfonos: **AppStore**, **GooglePlay** y **Marketplace**

RECOMENDACIONES

- **Comprobar el nombre de desarrolladores:** para comprobar la legitimidad de la aplicación.
  - **Comprobar el rating (puntuación):** para ver cómo está posicionada la aplicación.
- **Revisar los comentarios de otros usuarios:** para conocer sus opiniones y experiencias.
- **Leer la descripción de la aplicación y sus permisos:** para detectar engaños, faltas de ortografía que puedan hacernos dudar, permisos excesivos, etc.
- **Comprobar capturas de pantalla:** por si no cuadra con lo esperado o detectamos algo «raro».
- **Ver aplicaciones alternativas que ofrecen lo mismo:** si existen varias se recomienda elegir la que más puntuación y comentarios positivos tenga.
- **Visitar la página web del desarrollador:** para comprobar si ha desarrollado más aplicaciones y es de fiar.

RECOMENDACIONES

Estas recomendaciones son especialmente importantes si utilizas **markets alternativos**, ya que **permiten descargar aplicaciones no oficiales** y el riesgo de que sean fraudulentas es mayor.

el funcionamiento eS distinto:

- **Android: permite instalar aplicaciones de markets alternativos sin realizar cambios en el dispositivo.**
- **iOS: no permite instalar aplicaciones** de estos markets alternativos **a no ser que realicemos un Jailbreak** (proceso para sortear las restricciones del fabricante) al mismo.

MARKETS ALTERNATIVOS

ANDROID

- **Amazon Tienda Apps:** Contiene muchas aplicaciones gratuitas y de pago. Cada día regala una aplicación de pago.
- **Aptoide:** El más usado por personas que no pueden acceder a Google Play (por restricciones gubernamentales de su país).
- **F-droid:** Catálogo de aplicaciones gratuitas, algunas de código abierto.

IOS

- **Cydia:** para poder instalar aplicaciones de él, es necesario haber hecho **Jailbreak* al dispositivo. Contiene muchas aplicaciones y *tweaks* (permiten cambiar la apariencia del dispositivo y personalizar aspectos que Apple no permite).

**Jailbreak: proceso para acceder a todas las funcionalidades del dispositivo, saltándonos la limitaciones impuestas por Apple.*

OTROS ATAQUES QUE LOS DISPOSITIVOS PUEDEN SUFRIR

MALWARE:

Es importante **instalar un antivirus en los dispositivos móviles** que ayude a proteger tanto el terminal como la información almacenada en él.

- **Eset mobile Security** para Android.
- **NQ Mobile Security** para Android.
- **Lookout**: para iOS y Android.

PHISHING

- Es una **estafa**, en la que mediante un enlace o un mensaje fraudulento tratan de conseguir información confidencial como datos, claves, cuentas bancarias... engañando al usuario y haciéndole creer que está en el sitio correcto.

URL OCULTAS

Cuando navegamos por la web en nuestros dispositivos móviles no se muestra la url de la página. De esta manera, se ahorra espacio de pantalla pero también puede ser aprovechado para engañar a los usuarios y hacerles creer que están en una página que no es, siendo en realidad una copia fraudulenta.

- Algunos navegadores ocultan la url de la página.
- Otros la ocultan al desplazar la vista de la página hacia abajo.

ACORTADORES DE URL

Existen programas «acortadores» de URL, que sirven para condensar URL largas sin tener que copiarlas enteras, su uso se ha extendido en las redes sociales como Twitter, en las que el número de caracteres utilizados es muy importante.

ACORTADORES DE URL

¿Cómo puedo saber a qué dirección me están enviando estos enlaces acortados?

- **existen opciones para averiguarlo,** como por ejemplo:
  - **Redirect Checker**
  - **Unshorten.it**
  - **VirusTotal**

Pero lo importante es… NO HACER CLICK EN ENLACES ACORTADOS SI NO CONFIAMOS EN LA PROCEDENCIA DE LOS MISMOS.

JAILBREAK/ROOTEO DE DISPOSITIVOS

JAILBREAK

Se hace en dispositivos con **iOS** (Apple). Consiste en **eliminar las limitaciones impuestas por el fabricante en el sistema**, de manera que se puedan instalar apps y realizar acciones que no se podrían realizar de otro modo.

Permite:

- Instalar aplicaciones de terceros.
- Instalar temas y extensiones.
- Instalar tweaks.
- No permite acceso *root* (administrador) en el dispositivo.

ROOTEO

Consiste en **ganar** «acceso *root*» en un dispositivo, es decir, **permisos de súper usuario/administrador total.** Se hace en **Android** o sistemas basados en **Linux.**

Permite:

- Cambiar por completo el sistema operativo.
- Eliminar aplicaciones de fábrica.
- Aplicaciones especiales como usar VPN.
- Control sobre las aplicaciones instaladas.

PRACTICAS HABITUALES Y ARRIESGADAS EN LA EMPRESA

- **el uso compartido de tabletas**
- **dar de baja dispositivos sin borrar**

Para evitar los riesgos asociados a estas prácticas, es necesario:

- **Crear perfiles para cada uno de los usuarios que van a utilizar la tableta** para que la información se mantenga aislada en cada perfil.
- **Eliminar toda la información contenida en el dispositivo** antes de deshacernos del mismo (dárselo a otra persona, venderlo o desecharlo).

SEGURIDAD EN REDES WIFI

WiFi es una de las **tecnologías de comunicación inalámbrica** que más utilizamos hoy en día para conectar nuestros dispositivos a internet.

- Al tratarse de una conexión inalámbrica, **es fácil que un usuario malintencionado pueda interferir en nuestra comunicación y tener acceso a nuestra información.**
- **Procura evitar las wifis cuya configuración de seguridad desconozcas.**
- **A continuación veremos las amenazas a las que estás expuesto cuando usas wifis públicas y cómo configurar tu wifi para evitar intrusiones.**

SEGURIDAD EN REDES WIFI

AMENAZAS

Robo de información/sniffing (escucha)	**Una configuración deficiente de la red wifi, puede permitir a un atacante robar la información transmitida a través de la red.**
Conexión directa con nuestros dispositivos	Un atacante podría acceder a nuestros equipos conectados a la red y por tanto a toda nuestra información.
Vulnerabilidades conocidas	Tanto los routers, las contraseñas de algunas redes, el tipo de cifrado, o funcionalidades como WPS, son vulnerables, por lo que el atacante puede aprovecharse de ello para sacar partido.
Creación de redes «espejo»	Un atacante puede crear una red inalámbrica con el nombre de una red en la que el dispositivo confía para que éste se conecte. De esta manera, su comunicación y la información que contiene queda expuesta.
Redes públicas	Al conectar a redes ajenas a nuestra organización (hotel, aeropuerto,...), exponemos nuestros equipos a las posibles deficiencias de seguridad que pudieran existir.

RECOMENDACIONES PARA UNA SEGURA CONFIGURACIÓN DE REDES WIFI

- **Cambiar contraseña por defecto del router:** establecer una contraseña robusta y asociarla el cifrado más fuerte disponible en el momento.
- **Cambiar nombre de la red** (SSID/ESSID) **por defecto y ocultarlo** (no se mostrará a otros dispositivos) así evitaremos que alguien pueda intentar conectarse a la red.
- **Actualizar firmware del router:** las actualizaciones suelen incluir mejoras de seguridad.
- **Desactivar WPS:** un mecanismo que facilita la conexión de dispositivos a la red. Es vulnerable, y puede facilitar la conexión de terceros a la red.
- **Cambiar contraseña de acceso al panel de configuración del router:** las contraseñas son conocidas (se encuentran buscando en Google el modelo y fabricante), si un atacante puede acceder a este panel, podrá configurar el router sin restricciones.
- **Elige un protocolo de cifrado seguro:** utilizar en todo momento el protocolo de cifrado WPA2 que actualmente es el más seguro.

CONCLUSIONES

- **El mayor riesgo frente a los dispositivos móviles** no es el robo de información si no la **sustracción** de los mismos por el elevado precio demanda de algunos de los modelos. En este tipo de ataques, las información almacenada en el dispositivo no es el objetivo principal. Muchas compañías ofrecen seguros sobre los dispositivos.
- A través de nuestros dispositivos móviles **podemos sufrir los mismos tipos de ataques que a través de los ordenadores conectados a redes cableadas**. Además tienen riesgos específicos asociados a las **nuevas funcionalidades** que incorporan, como los mecanismos de localización vía GPS o los protocolos de comunicaciones wifi, NFC y Bluetooth.

CONCLUSIONES

- Existen distintas **medidas para evitar el acceso al dispositivo** por terceros en caso de sustracción lo que permite proteger el acceso a la información del mismo. Las pérdidas de información también pueden evitarse a través de copias de seguridad.
- Las **copias se seguridad**, son copias de respaldo o *backups* de la información almacenada en el teléfono, que nos garantizan poder recuperar la información importante (contactos, fotos,…) en caso de que surja un imprevisto. Se pueden realizar en local o en la nube.
- WiFi es una de las tecnologías de comunicación inalámbrica que más utilizamos hoy en día para conectar nuestros dispositivos a internet. Al tratarse de una conexión inalámbrica, es fácil que un usuario malintencionado pueda interferir en nuestra comunicación y tener acceso a nuestra información. **Procura evitar las wifis cuya configuración de seguridad desconozcas.**

FUNDACIÓN DE EDUCACIÓN SUPERIOR
SANJOSÉ
INSTITUCIÓN TECNOLÓGICA

FIN DE GRABACIÓN