AF4: Seguridad en la red

Seguridad en terminales móviles: configuración y copias de seguridad

Digitalización aplicada al sector productivo.
Módulo formativo sobre competencias digitales transversales básicas.

Proyecto financiado por el Ministerio de Educación y Formación Profesional - *U.E. Next Generation*

Índice

1. INICIO

1.1 Introducción

Los teléfonos móviles se han convertido en uno de los blancos favoritos de los ataques de ciberdelincuentes: la gran cantidad de datos, documentos, vídeos y fotografías que se almacenan en ellos, los hacen particularmente interesantes.

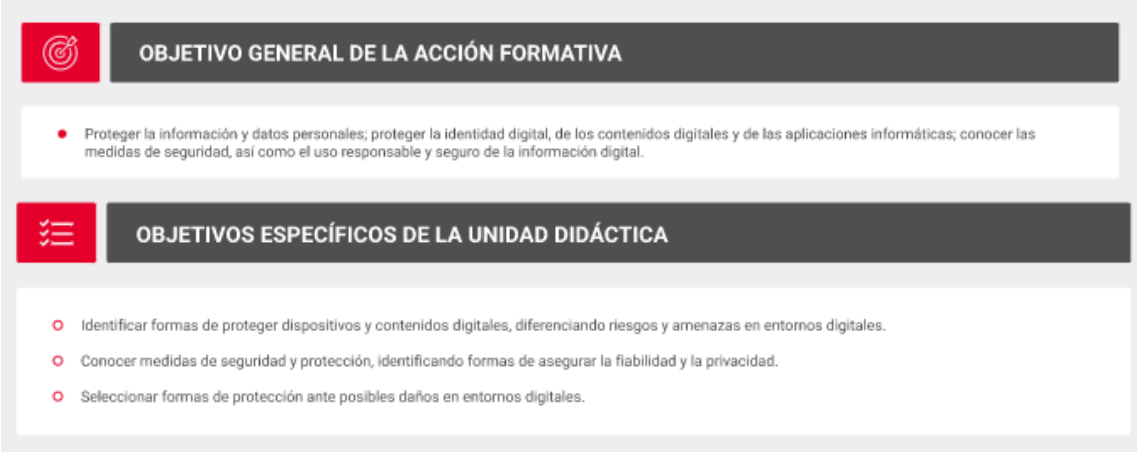
Los teléfonos te acompañan diariamente, simplifican las actividades laborales y permiten tener la información que se necesita. El lado negativo de estas ventajas es que, si caen en las manos equivocadas, también pueden brindar infinidad de datos que tienes almacenados a posibles **ciberdelincuentes**, exponiéndote a grandes riesgos.

En esta Acción Formativa conoceremos a Marta, una chica de 25 años, trabajadora social de la ONG "Un mundo mejor". Ella tendrá que manejar mucha información confidencial, datos personales, informes de familias en riesgo y expedientes que requieren la protección de la información.

La ONG también es consciente de la importancia de resguardar los datos y la información, en muchos casos confidencial, de las personas con las que trabaja y por eso, pone las medidas que están a su alcance para protegerlos, ya que es su responsabilidad.

En esta Unidad Didáctica podrás ver como Marta tratará las posibles **amenazas** por las que se puede ver afectada. No solo la información laboral que maneja, sino también la suya propia. Conocerá **cuáles son las precauciones** que debe tener con el teléfono móvil para proteger la información personal y la de sus contactos. Aprenderá a ser precavida con las aplicaciones que se instala y conocerá algunos buenos hábitos en cuanto a seguridad para proteger la información personal y laboral. Finalmente, conocerá cómo protegerse ante las aplicaciones que buscan infectar y robar la información de los teléfonos móviles (*malware*).

¿Qué vas a aprender en esta unidad?



2. PROTECCIÓN DEL TERMINAL MÓVIL

2.1 Amenazas en los terminales Móviles

"Las ciberamenazas evolucionan rápidamente; son cada vez más complejas y adaptables. Gracias a los requisitos que introducimos hoy, mejoraremos considerablemente la seguridad de una amplia gama de productos y reforzaremos nuestra resiliencia frente a las ciberamenazas, en consonancia con nuestras ambiciones digitales para Europa". Thierry Breton, comisario de Mercado Interior.

Cuando hablamos de **amenazas en los terminales móviles** nos referimos a toda **actuación o fallo de seguridad** en los dispositivos móviles que puede suponer la **pérdida o robo de los datos**, con los consiguientes daños o inconvenientes que esto puede provocar tanto a nivel personal como laboral.

Hoy la mayoría de las personas tenemos un teléfono móvil que se conecta a internet constantemente. Estos dispositivos inteligentes han pasado a ser parte esencial de nuestra vida: enviamos mensajes, redactamos correos electrónicos, trabajamos en ellos, realizamos compras, hacemos videollamadas y muchas cosas más.

Debemos ser conscientes de las amenazas que afectan a estos dispositivos y tomar las **precauciones necesarias para protegerlos** para evitar poner en riesgo los datos e información personal o relativa a nuestro trabajo.

A continuación, vamos a repasar **algunos de los contenidos más comunes** que guardamos en nuestro teléfono móvil y la **valiosa información que de ahí pueden extraer los ciberdelincuentes.**

Contactos y datos personales

A menudo, cuando pensamos en los contenidos de nuestro teléfono móvil, lo primero que se nos viene a la cabeza es la información de nuestros contactos que brindan una información extremadamente valiosa sobre las personas y las redes de conexión que existen entre ellas, pero además de los contactos, tu teléfono móvil, ya sea personal o de trabajo, almacena una **gran cantidad de información que dice mucho de tu persona**.

Información sobre la vida personal
Como por ejemplo la relación laboral, familiar o personal con cada uno de tus contactos, así como fotos o imágenes privadas.

Cargo profesional
Por ejemplo, a través de los correos electrónicos de tu trabajo es posible averiguar tu lugar de trabajo y cargo que desempeñas.

Gustos de consumo
Si alguna vez has comprado algo por internet, tus preferencias de consumo ya están identificadas y sería muy fácil descubrirlas a partir de tu móvil.

Tendencias políticas
Tus opiniones pueden quedar reflejadas en una red social a la que accedes desde una app que te has descargado o a partir de las conversaciones que hayas podido mantener WhatsApp.

Grupos de trabajo/ocio en los que se participa
Los correos electrónicos de trabajo, las aplicaciones de gestión de tareas o incluso las conversaciones que puedes mantener con las personas con las que trabajas revelan mucha información en este sentido.

Situación socioeconómica
Por ejemplo, si tienes instalada alguna aplicación de gestión bancaria, ya sería muy sencillo averiguar tu situación socioeconómica en caso de robo o ataque.

Con la obtención de estos datos, quienes realizan actividades delictivas podrían identificar nuevas víctimas o emplear esta información para extorsionar y estafar.

Fotografías, vídeos y documentos

En el teléfono móvil **almacenamos una gran cantidad de información en forma de archivos**, quizás los que más apreciamos sean las bibliotecas de imágenes y videos

Pero no debemos olvidar que además de las fotos y videos, todos **los ficheros que adjuntamos a través de las aplicaciones de mensajería**, como los gestores de correo electrónico o *whatsapp*, también se almacenan en el móvil y que, en muchas ocasiones, contienen información que, si cayera en manos de ciberdelincuentes, podría **generar un gran daño o perjuicio.**

En el caso de Marta, que tiene la aplicación de gestión de correo electrónico que utiliza en su trabajo instalada en su móvil personal, es preciso que tanto ella como la ONG para

la que trabaja tomen las **medidas preventivas adecuadas para no comprometer la información relativa a las personas con las que trabajan** ante un posible ataque o robo del dispositivo.

Muchas personas acceden al correo electrónico a través del teléfono móvil, por lo que el riesgo del robo de datos debido a una intrusión no autorizada al dispositivo también ha aumentado. Es necesario tomar medidas para prevenir este tipo de intromisiones cuyo único objetivo final es extraer grandes cantidades de información y generar estafas.

2.3 ¿Qué hacer para proteger nuestro correo electrónico?

Los correos electrónicos son una vía de exposición para la ciberdelincuencia, por lo que es muy importante **corroborar la información** que recibes, **prestar atención** a los datos de la persona remitente y cerciorarse de que se trata siempre de una **fuente oficial**.

Si dispones de un teléfono de empresa y uno personal, te recomendamos que gestiones el email del trabajo en el teléfono de empresa y el email personal en tu teléfono móvil.

A continuación, te presentamos algunas sugerencias para proteger tu correo electrónico.

Factor de autenticación
Además de utilizar tu contraseña, usa un doble factor de autenticación que lo puedes realizar configurando la seguridad de tu punto de acceso en dos pasos (contraseña y envío de código a tu teléfono móvil).

Contraseña
Utiliza una contraseña segura para acceder al punto de entrada de tus correos.

Dispositivos seguros
Si vas a iniciar sesión hazlo siempre en un dispositivo seguro con protección contra virus y ciberamenazas

Cerrar sesión
Es recomendable cerrar tu sesión de correo en los distintos dispositivos.

Prestar atención
Es muy importante cuidar el tipo de correo electrónico que abres. No abras aquellos correos dudosos o que llegan a la zona de "*spam*" o correos no solicitados.

2.2 Recomendaciones para mantener seguro el terminal móvil

Los teléfonos móviles se han convertido en herramientas de trabajo esenciales que contienen una gran cantidad de información personal y laboral. Por esa razón es imprescindible tomar algunas precauciones para protegerlos y salvaguardar la información que almacenan.

Marta empieza a ser consciente del valor que tiene su teléfono móvil, ya no solo como herramienta de trabajo, sino también por la **cantidad de información que almacena**. Desde su móvil es posible acceder a sus contactos, a sus correos electrónicos, aplicaciones de trabajo, conversaciones... ¡Todo!

A Marta le tranquiliza que la ONG para la que trabaja también es consciente de este hecho y toma **medidas de ciberseguridad** necesarias como la **instalación y actualización periódica de programas antivirus** específicos para los terminales móviles de sus profesionales, así como la **solicitud de autentificaciones de perfiles mediante contraseñas robustas** a la hora de acceder a las cuentas de correo electrónico y gestores de tareas.

Sin embargo, le gustaría tomar nota de algunas **recomendaciones para mantener seguro su móvil** y proteger la información que almacena.

Realiza copias de seguridad

Haz periódicamente copias de seguridad de los datos que guardas en el teléfono. Así, si pierdes el teléfono seguirás teniendo acceso a tu información personal.

Utiliza contraseñas complejas

Utiliza diferentes contraseñas para cada servicio e intenta que sean difíciles de descifrar.
Las contraseñas como 0000, 1234 o tu fecha de nacimiento son un clásico que quienes cometen actos delictivos van a probar si intentan acceder a tu teléfono u ordenador.

No conectarse a redes públicas o abiertas

Muchos lugares públicos nos permiten acceder de manera gratuita y abierta a sus redes wifi. Sin embargo, esto es peligroso, ya que te expones a que tu dispositivo sea vulnerado por delincuentes.

Bloquea tu teléfono

Configura tu teléfono para que se bloquee automáticamente cuando no lo utilices. Según el tipo de teléfono, se puede utilizar un pin, un código de acceso, la huella digital o la retina del ojo

Mantén actualizados los programas

Activa las actualizaciones automáticas de tu teléfono para que se subsanen fisuras de seguridad.

Activa la ayuda para localizar el teléfono

En caso de pérdida, muchos teléfonos tienen un programa que permite localizarlo, borrar los datos en remoto o bloquearlo, de modo que se garantice su seguridad.

Desactiva las conexiones que no uses

Existen tipos de conexiones como el *bluetooth* o el punto de acceso personal que en algunas ocasiones habilitamos para poder conectarnos a otros dispositivos como relojes inteligentes o un ordenador portátil. Desactiva este tipo de conexiones cuando no las utilices y así no crearás una brecha de seguridad en tu teléfono.

Desactivar las conexiones que no se utilicen en los dispositivos

Antiguamente, la conexión ***bluetooth*** se utilizaba en pocas ocasiones. Sin embargo, el uso generalizado de ***wearables,*** o dispositivos que se llevan puestos, hace que cada vez más se utilice este tipo de conexión. Los auriculares, los relojes o los altavoces inteligentes necesitan conectarse por vía *bluetooth*.

Como recomendación general, es conveniente que cuando no estés usando esta conexión, no se mantenga activada. Es especialmente importante atender esta recomendación cuando nos encontramos en espacios con mucha concentración de dispositivos, como pueden ser centros comerciales u hoteles, porque si tienes habilitada la conexión *bluetooth* es muy fácil que accedan a tus propios dispositivos.

No es conveniente realizar conexiones a redes públicas o abiertas

Muchas cafeterías y restaurantes ofrecen la posibilidad de utilizar su conexión wifi a los clientes, pero cuando nos conectamos a una red pública, abierta o gratuita no conocemos quién la administra, por lo que podemos exponernos a diferentes riesgos tales como:

- **Robo de datos transmitidos.** Cuando la red es abierta cualquier perfil de administrador de la red o incluso persona usuaria puede leer los datos con los que trabajamos.
- **Robo de datos almacenados.** Una brecha de seguridad puede dejar nuestros dispositivos al descubierto y se puede producir el robo de la información guardada en ellos.
- **Virus.** Nuestro dispositivo queda más expuesto a la entrada de virus.

Con las **conexiones a internet a través de redes wifi-públicas o abiertas**, hay que ser especialmente precavidos porque surgen principalmente dos **problemas de seguridad** a considerar:

- Existen muchas posibilidades de que se produzcan **brechas de seguridad** que facilita el acceso a los datos almacenados en el móvil o transmitidos a través de la red.

- La compañía que proporciona la red pública **podría solicitar algunos datos** de la persona usuaria a cambio de hacer uso de la red wifi y en este caso, **se cederían datos personales** a la empresa proveedora de la red. A partir de ese momento, la empresa podría comenzar a enviar sus campañas publicitarias a estas personas o incluso hacer negocio con los datos personales recopilados con otras compañías.

Una vez que ya conoces los riesgos a los que te puedes exponer, antes de contactarte a internet a través de una wifi pública, piensa si te compensa. No siempre el tiempo que vamos a utilizar internet merece afrontar el peligro que suponen este tipo de redes.

2.3 Configuración de terminales móviles y copia de seguridad

Configuración de terminales móviles

Las compañías que desarrollan los principales **sistemas operativos** de terminales móviles, conscientes de la importancia de prevenir riesgos relacionados con la seguridad, ofrecen, en la mayoría de las versiones, **opciones de configuración** que es conveniente activar para proteger el dispositivo y, por tanto, la información que almacena.

A Marta le va a venir muy bien conocer estas opciones de configuración relacionadas con la seguridad de su dispositivo.

Configuración de seguridad para teléfonos con sistema operativo Android

Si tienes un teléfono móvil iPhone puedes **configurar tu dispositivo** según las indicaciones que se presentan en el siguiente video.

A continuación, si tienes un teléfono móvil con sistema operativo Android, revisa el siguiente video para ver **cómo puedes configurarlo** con un mayor nivel de seguridad.

Utiliza las opciones de configuración que te ofrece el terminal móvil, cuanto más restrictivos sean los accesos a las aplicaciones que tengas instaladas, mayor seguridad estarás otorgando a tu móvil y a los datos que en él almacenas.

"Una copia de seguridad es el duplicado de un archivo informático que se guarda para prevenir la pérdida o destrucción del original".
Real Academia Española (RAE)

¿Por qué es necesario hacer copias de seguridad?

Los **robos**, **extravíos** o **roturas** de teléfonos móviles son bastante comunes, por eso es conveniente mantener los datos salvaguardados, bien mediante una **carpeta en línea con la que se sincroniza lo más importante o bien mediante una copia de seguridad** para que puedan recuperarse en caso de que haya algún problema con el dispositivo.

Las copias de seguridad van a permitir **recuperar la información desde la última copia** en caso de que sea necesario, lo único que necesitas es ser constante y hacerlas periódicamente o, en su defecto, programar copias de seguridad automáticas en los dispositivos.

¿Cómo hacer una copia de seguridad de los datos del teléfono móvil?

Las **copias de seguridad de los datos que guardas en tu teléfono móvil** puedes enviarlos a diferentes espacios, como por ejemplo un ordenador, un disco duro externo, un servidor web u otra empresa que utilice soporte de almacenamiento que no sea la que viene por defecto en tu dispositivo.

Una manera muy efectiva de almacenar las copias de seguridad de forma automática desde tu móvil es llevándolos a la **"nube"** o espacios de almacenamiento en internet. Aquí lograrás proteger todas tus aplicaciones, contactos, mensajes de chat, imágenes y demás información que tengas en el móvil.

Protege tu información confidencial antes de deshacerte de tu teléfono móvil.

Se estima que la vida media de un móvil son solo 15 meses, por lo que **es habitual deshacernos de ellos con cierta frecuencia**. También puede ocurrir que el móvil se averíe y tengamos que llevarlo al servicio técnico. En todos estos casos, la **información privada quedaría expuesta**.

Quizás nunca has reparado en la información que se queda almacenada en tu dispositivo y a la que podrían acceder otras personas, por esta razón, te damos varios consejos de utilidad:

Haz una copia de seguridad

Antes de tirar, reciclar o llevar a reparación tu teléfono, haz una copia de seguridad de todos los datos y documentos que tengas guardados. Nunca sabes cuándo puedes necesitar recuperar alguno.

Retira las tarjetas SIM y SD

Retira las tarjetas que tengas guardadas. Si vas a cambiar de compañía o número de teléfono es conveniente destruir la SIM antigua. Recuerda que la **tarjeta SIM** es la que te facilita tu compañía de teléfono y te asigna un número, por otro lado, la **tarjeta SD** es la tarjeta de memoria externa en la que se puede almacenar la información

Borra tu información personal

Tras hacer una copia de seguridad, elimina la información de tus contactos, los mensajes, las fotografías, los documentos confidenciales, los vídeos, los chats de mensajería instantánea, las contraseñas y claves de accesos a los servicios instalados, el historial de búsqueda de navegación o las notas que has creado. Puedes optar por restaurar el móvil a sus valores de fábrica de modo que se borre toda información guardada.

Deshabilita los accesos a tus cuentas

Cuando tires, regales o lleves a servicio técnico tu teléfono es fundamental que desactives el acceso a tus cuentas de correo y las contraseñas a los servicios instalados, así como las de conexiones wifi.

Desvincula también tu teléfono de otros dispositivos que estén vinculados.

Al borrar y restaurar el dispositivo a valores de fábrica, te pedirá que desvincules otros dispositivos o desactives alguna aplicación.

En el apartado **referencias bibliográficas** podrás encontrar información clara y útil para realizar estas acciones en tu teléfono.

Los dispositivos móviles, además de tener una duración determinada, están sujetos a desperfectos, caídas, robos y extravíos. Por todo esto, hacer una copia de seguridad te garantiza salvaguardar la información que tienes almacenada en el mismo.

3. PRINCINCIPALES FRAUDES Y RIESOS

3.1 Aplicaciones fraudulentas que suplantan a aplicaciones conocidas

Una de las fórmulas más usadas por ciberdelincuentes para lograr que se instale su aplicación fraudulenta en los teléfonos móviles es la réplica hasta el mínimo detalle de una aplicación conocida.

Ejemplo: suplantación de la app de BBVA

En 2020, el banco **BBVA advertía de la suplantación fraudulenta de su aplicación** y difundió el aspecto y el modo en el que la versión falsa solicitaba los datos bancarios para que toda su clientela conociera la estafa y no cayeran en la trampa.

Con esta táctica no solo **robaban datos a la clientela del BBVA,** sino también **infectaban sus móviles**. El riesgo de equivocarse era muy alto pues la falsificación era muy parecida a la real.

Generalmente, este tipo de aplicaciones fraudulentas, que nos podemos instalar creyendo que son auténticas, sirven para recabar datos bancarios, aunque también suelen instalar software malicioso que provocan cambios en el funcionamiento del terminal, ralentizando la actividad del móvil.

Algunas recomendaciones para evitar aplicaciones

Siempre es recomendable ir a las tiendas oficiales a la hora de descargarte una aplicación y no desde páginas web.

La gran ventaja de las tiendas oficiales frente a otras opciones es que los dos sistemas operativos más extendidos, iOS de Apple y Android de Google, **realizan controles sobre las aplicaciones**, lo que permite a las personas usuarias tener cierta seguridad respecto a la aplicación que desea instalar

Tiendas oficiales más conocidas.

Google Play

Se trata de la tienda oficial para los dispositivos con sistema operativo Android. Haciendo clic en el ícono, se puede acceder a la tienda, buscar la aplicación deseada, consultar sus características y hacer clic en "Instalar" para utilizarla en el dispositivo.

App Store

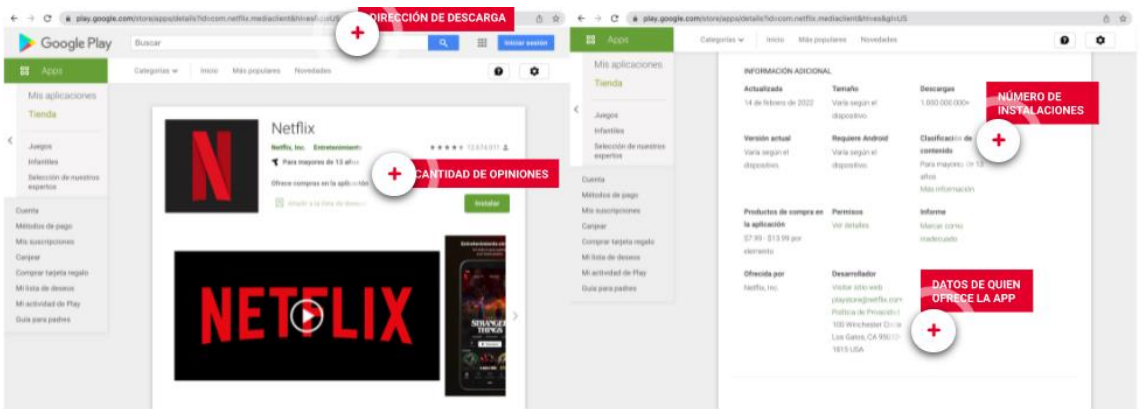
Es la tienda de aplicaciones gestionada por Apple. En los dispositivos con sistema operativo iOS se puede acceder haciendo clic en el ícono, buscar la aplicación que se desea y hacer clic en "Obtener". A continuación, se deberán ingresar el ID y contraseña si el sistema lo solicita y finalmente, instalar la aplicación.

Desconfía de los enlaces para descargar una aplicación que te lleguen por correo electrónico o desde una web de la que no tienes conocimiento: descargar una aplicación desde un enlace es mucho más inseguro que hacerlo desde la tienda oficial del sistema operativo.

Es aconsejable ser precavidos a la hora de instalarnos aplicaciones relacionadas con entidades bancarias o redes sociales.

¿Cómo distinguir una aplicación oficial de una aplicación fraudulenta?

Existen algunas señales que nos permiten **identificar si la aplicación se trata de una versión oficial** o si estamos ante un caso fraudulento:



Dirección de descarga
Algo a lo que debes acostumbrarte es a **mirar la dirección** antes de proceder a realizar ninguna descarga. Si observas que no estás en la web de la compañía o en la propia aplicación de descargas del sistema operativo, debes evitar continuar

Cantidad de opiniones
Una aplicación muy popular, a diferencia de una aplicación fraudulenta, suele contar con muchas opiniones de las personas usuarias que ya la han utilizado anteriormente.

Las mejores aplicaciones suelen estar en los primeros puestos de las tiendas oficiales.

Número de instalaciones

Las aplicaciones populares, como pueden ser las redes sociales, las de banca online o los servicios de contenidos audiovisuales, tienen un alto número de instalaciones. Si la aplicación parece muy conocida pero el número de instalaciones es bajo, no resulta fiable.

Datos de quien ofrece la app

Por lo general, las empresas ofrecen las aplicaciones bajo el nombre de las marcas. Se debería desconfiar especialmente de una app donde el nombre de su fabricante no coincida con la empresa o con algún servicio de desarrollo de aplicaciones oficial reconocido.

Las aplicaciones en nuestro día a día

Quizá estés pensando que tú eres de las personas que no necesita tener en cuenta estas recomendaciones, ya que habitualmente no descargas aplicaciones en tu móvil. Sin embargo, cada vez dependemos más de su uso, a veces obligatorio, para realizar gestiones administrativas habituales.

Por ejemplo, las administraciones públicas nos piden, cada vez más, que **cambiemos la forma de hacer las gestiones y determinados trámites** y pasemos del modo presencial a un modelo digital.

Una de las herramientas que ponen a nuestra disposición es la aplicación **Clave PIN** para poder acceder y ejecutar muchos trámites.

Piensa bien qué aplicaciones necesitas en el móvil, porque tener una gran cantidad de aplicaciones instaladas hace que el funcionamiento del dispositivo se ralentice. Normalmente, solo se utiliza un pequeño número de aplicaciones de la gran cantidad que han sido instaladas.

3.2 "Malware" para terminales móviles

Malware son aplicaciones maliciosas que tratan de tomar el control completo del dispositivo. Son las más peligrosas.

Ejemplo: FaceApp, la app de la polémica

En 2019, la polémica acerca de los **datos que cedemos cuando nos damos de alta en una aplicación** se hizo muy evidente cuando *FaceApp*, la aplicación que aplicaba un filtro sobre tus imágenes para ver tu apariencia en edad anciana encubría una **política de privacidad muy opaca.**

Entre los términos de uso, las personas usuarias cedían su información personal y el acceso a sus fotografías, pero también concedían la monitorización de su actividad web, su ubicación y compartir la información que recogía la aplicación con una jurisdicción diferente del país de origen.

Ejemplo: el negocio fraudulento en torno a Pokemon Go

En 2016, el juego para móviles *Pokemon Go* causó una verdadera fiebre. Esta popularidad provocó el interés de **delincuentes que encontraron en esta aplicación una fuente para cometer estafas**, hacerse con los datos personales para suplantar identidades y crear ciberataques para conseguir el control de dispositivos ajenos.

Fue tal la expectativa alrededor del juego, que ya un par de días antes de su lanzamiento al mercado **existía otra App pirata** con el mismo nombre cuyo objetivo era secuestrar el teléfono, sustraer información privada, monitorizar su uso y hacerse con el control de algunas funcionalidades como el GPS y la cámara de fotos o el micrófono.

El *malware* está diseñado para formar parte de nuestro conjunto de aplicaciones y generalmente suelen ser aplicaciones gratuitas de apariencia inofensiva. Sin embargo, pueden llegar a ser extremadamente dañinas, ya que, sin darnos cuenta, les concedemos el permiso para acceder a la cámara, al micrófono u otras funciones del dispositivo, pudiendo tomar fotografías sin consentimiento o grabar conversaciones.

Algunas recomendaciones para evitar malware

Es aconsejable mantener un control riguroso de las instalaciones que tenemos en el dispositivo y eliminar aplicaciones que no usemos a menudo, especialmente si no la hemos descargado desde una página oficial.

Una buena recomendación es identificar en los ajustes del dispositivo las **aplicaciones a las que se les ha dado permiso** para utilizar la cámara, el micrófono, información sobre la ubicación, conexión a los datos móvil o para acceder a las carpetas del terminal.

En caso de que se observe alguna aplicación que haya solicitado algún tipo de **acceso sin que le corresponda según sus funciones** deberíamos desconfiar de ella.

¿Qué hacer si el dispositivo ha sido infectado por un malware?

Si se siguen las precauciones de seguridad, los dispositivos deberían mantenerse a salvo de virus. Sin embargo, es posible que de todos modos se haya instalado un *software malicioso* y nos encontremos ante la necesidad de eliminarlo de nuestro dispositivo móvil. En este caso existen tres alternativas:

Antivirus:

Instalar un antivirus de fabricante reconocido, buscándolo en tiendas oficiales, y luego hacerlo funcionar para detectar la aplicación peligrosa.

Probar manualmente:

Si el antivirus no funciona, se puede probar eliminar el virus manualmente: En este caso veremos cómo eliminar el *malware* de un sistema operativo de Android.
En primer lugar, se deberá activar el modo seguro desde **Configuración**. Luego ir a **Ajustes**, enseguida a **Aplicaciones** y por último, a **Aplicaciones descargadas**. Haz clic en **"Desinstalar"** sobre aquella aplicación que ha comenzado a generar inconvenientes.

Si esta acción no tiene éxito, se puede intentar ir a **Ajustes**, luego a **Seguridad** y a continuación a **Administradores de dispositivos**. Haz clic en **"Desactivar"** la aplicación, para luego intentar desinstalarla nuevamente.

Consulta a expertos:

Si no se puede desinstalar la *app,* es recomendable que consultes con una **persona experta** para que pueda ayudarte a encontrar una solución. De lo contrario, será necesario hacer una restauración de fábrica borrando todos los datos del teléfono móvil (incluyendo la aplicación maliciosa) para poder volver a utilizarlo con normalidad.

El *malware* es uno de los ataques más peligrosos que podemos sufrir en los dispositivos móviles.

3.3 Troyanos y "Ransomware"

Los troyanos son programas que, haciéndose pasar por otros, engañan a las personas usuarias para tomar el control de sus dispositivos.

Como ejemplo, podemos mencionar el Emotet , uno de los troyanos más activos en nuestro país. Emotet funciona como un troyano bancario, este troyano llega a los equipos mediante campañas de spam en archivos adjuntos o mediante hipervínculos en el propio cuerpo del correo electrónico.

Un troyano es un **programa o aplicación aparentemente legítima y segura** que, al introducirse y ejecutarse en el móvil, permite a quien realiza el ataque **acceder al dispositivo infectado y controlarlo en remoto**, permitiéndole, por ejemplo, mandar mensajes en nombre de la persona propietaria del móvil o cualquier otra acción.

Los troyanos están muy extendidos entre los ordenadores y han empezado a operar con fuerza en los dispositivos móviles. Este tipo de aplicaciones puede realizar diversas acciones fraudulentas, pero su característica principal es que siempre aparecen "camufladas" debajo de una aplicación que funciona de forma legítima.

¿Cómo actúa un troyano?

Consigue el control
Para poder hacerse con el control de alguna función del sistema, los troyanos solicitan permiso al usuario o la usuaria, cumpliendo con los requisitos del sistema operativo.

Accede a funciones
Una vez que le has dado el permiso accede a las funciones de tu dispositivo y se instala provocando un rendimiento anómalo en su funcionamiento como por ejemplo: cierre de las aplicaciones inesperadamente o instalación de aplicaciones sin autorización.

Ataca al dispositivo
Una vez que accede al dispositivo, el troyano puede ejecutar el ataque eliminando, borrando o bloqueando los archivos y la información.

¿Sabías que...?

Los troyanos toman su nombre de la leyenda de "El Caballo de Troya", ya que utiliza la estrategia de ocultarse bajo una apariencia inofensiva para que, una vez dentro de su objetivo, pueda realizar el ataque. Puedes conocer más sobre esta leyenda accediendo a Wikipedia.

El *ransomware es* un tipo de *malware* que suele tener una intención clara de chantaje económico. Su forma de operar es congelar los archivos del dispositivo, cifrándolos para que no se pueda acceder a ellos y solicitar después un “rescate” para devolverlos.

Ejemplos de ransomware famosos

A continuación, te mostramos algunos **métodos** que utilizaron algunos de los *ransomware* más significativos que actuaron en el pasado.

TeslaCrypt
El programa infectado se escondía en archivos anexos a ciertos videojuegos.

SimpleLocker
Atacaba al sistema operativo de los teléfonos Android dificultando el acceso de las víctimas a la interfaz del dispositivo. Tenía formato de app y accedía a la cámara de fotos.

WannaCry
Malware que atacó a empresas, instituciones y organizaciones a nivel mundial a través de brechas de seguridad que le permitían colarse en los dispositivos conectados en red. Fue un caso tan importante que saltó a los medios de comunicación.

Cryptolocker
Se transmitía en archivos adjuntos y mensajes spam a través de otro troyano, el GameOver Zeus, que infectaba a ordenadores para que fueran parte de una red que era controlada de forma remota, denominada botnet. Esto hacía que la infección de cryptolocker fuera muy rápida, encriptando los datos del dispositivo.
La víctima debía pagar para recuperar sus archivos

SamSam
Accedía a los dispositivos a través de contraseñas débiles o fácilmente vulnerables, escaneaba la red de la víctima, habitualmente empresas, infectando el sistema, encriptando la información y solicitando un rescate.

Cerber
Se ocultó en un documento de Microsoft Office remitido por correo para expandirse a través del paquete en la nube de Office 365.

Los ataques de tipo *ransomware* se suelen extender habitualmente a través de los ordenadores, sin embargo, en los últimos tiempos también han llegado a los teléfonos móviles ante la gran cantidad de información valiosa que los nuevos dispositivos permiten almacenar

¿Cómo funciona?

Su fórmula más común para extenderse es **el correo electrónico** y sus fases suelen ser siempre las mismas:

Descarga del programa

Todo comienza cuando el usuario o usuaria descarga el programa o la app que da inicio al proceso.

El secuestro

Una vez que el *ransomware* se ha instalado en el dispositivo, actúa cifrando los datos y los hace inaccesibles para su dueño o dueña. A partir de ese momento, se necesitará una clave para poder recuperar la información que poseía en el dispositivo.

El chantaje

Aparece una ventana en la pantalla con las instrucciones de pago. Dependiendo del dispositivo, también puede aparecer un archivo con instrucciones o un mensaje. En dicha comunicación el o la ciberdelincuente solicita un pago para el envío de una clave que ayudará a la víctima a recuperar sus datos.

Normalmente la petición tiene un límite de tiempo y se amenaza al usuario o la usuaria con destruir para siempre los datos si no realiza el pago.
Aquí es donde la persona puede decidir si afrontar el pago o no.

El rescate

Si la persona decide pagar, se concreta la última fase. Es posible que luego del pago se reciba la clave (ya que para el o la ciberdelincuente es un negocio), pero se han dado varios casos en los que dicha clave nunca ha llegado al usuario después de haber realizado el pago.

No todos los *ransomware* piden directamente un rescate. Hay algunas variantes que se hacen pasar por una autoridad policial, solicitando que se pague una multa, o por una

empresa de seguridad que informa de la necesidad de comprar inmediatamente un antivirus para recuperar el control del dispositivo.

Los métodos para engañar a la víctima son variados y cada vez más sofisticados, por lo que, antes de abrir un correo electrónico de origen desconocido, acceder a un enlace sospechoso, descargar un archivo adjunto, instalar una aplicación o conceder tus datos personales, debes estar alerta para evitar que el ransomware se instale en tu móvil.

¿Cómo actuar ante un ataque de ransomware?

Los ataques de tipo *ransomware* suelten tener una gran repercusión porque habitualmente **perjudican a las organizaciones y compañías**, realizando robos de datos altamente valiosos. Es por ello que cada vez más, las organizaciones y empresas **implementen sistemas de ciberseguridad en sus negocios y objetivos**, pues son conscientes de que un ataque de estas características podría costarles muy caro.*:*

Hace unos años la ONG "Un mundo mejor" fue víctima, junto con otras instituciones, de un ataque cibernético de tipo *ransomware*. La terrible experiencia les hizo tomar conciencia de la importancia de implementar sistemas de ciberseguridad para evitar este tipo de ataques.

En aquella ocasión la ONG supo actuar con éxito y no cedió al chantaje económico, pero manejar este tipo de situaciones no es nada fácil, sobre todo si no existen sistemas de ciberseguridad implementados en la compañía.

Como recomendación general, cuando el *ransomware* ha afectado el dispositivo, lo más **adecuado es apagarlo** para evitar que el virus se siga propagando y dar aviso a las autoridades policiales. Si no se cuenta con una copia de seguridad, se puede **recurrir a empresas especializadas en recuperar información encriptada o herramientas online que permiten identificar el tipo de ataque y recomendar una solución**.

Si bien es comprensible sentir desesperación y **buscar una solución inmediata**, en **ningún caso se recomienda hacer un pago a los o las cibercriminales**, además de que **ese pago no garantiza la devolución de los datos.**

Es responsabilidad de las empresas e instituciones garantizar la seguridad de la información tanto de las personas a las que ofrecen sus servicios, como de las personas que trabajan dentro de la propia organización.

3.4 "Smishing" y cómo evitarlo

El smishing es un tipo de engaño que consiste en hacerse pasar por una web con una identidad corporativa a la que está suplantando mediante un SMS o servicio de mensajería.

Ejemplo: Suplantación Netflix

En 2017 Netflix fue víctima de una estafa remitida por mensajería instantánea. En esta ocasión, se ofrecía una suculenta promoción a través del acceso a un enlace sospechoso.

Si prestas atención a los detalles, verás en la imagen que el enlace de acceso es extraño. Una dirección web correcta siempre tiene una estructura básica: después del **https: //** y antes de la primera barra (/), **debe incluir el nombre de la empresa** y después la ruta.

En este caso, la web pirata es **Wp5.co** y trampearon el acceso para generar confusión añadiendo al final la palabra netflix.

Este fraude se basa en **enviar un mensaje con la apariencia de una organización o entidad reconocida** en el que se ofrece un acceso donde al final la víctima introducirá sus datos personales. Suele ser común que estas técnicas se hagan pasar por un portal donde se piden el **nombre de la persona usuaria y la contraseña** para acceder.

En el propio mensaje pueden aparecer frases como: "para realizar el cambio ha de acceder a nuestra página introduciendo sus datos". **El problema es que la página no corresponde a la empresa, sino a las personas que están realizando la estafa.** Al introducir sus datos en esa página se les facilita tanto el nombre de usuaria o usuario como la contraseña del servicio.

Se debe tener especial cuidado con este tipo de estafas, ya que pueden acceder a nombres de usuario o usuaria y claves de mucha importancia.

Marta no lo sabe, pero está a punto de ser ser víctima de *smishing* a través de un aparentemente inocente mensaje de SMS. Veamos qué le ocurre y cómo resuelve la situación.

Una notificación inesperada

Suena un aviso de SMS de teléfono móvil y Marta recibe un mensaje que no esperaba. Aunque el remitente es desconocido, lee el SMS extrañada:

"¡Vaya! Acaba de llegar un SMS a mi teléfono para recoger un paquete, pero no recuerdo haber realizado ninguna compra recientemente. Quizás sea un envío que me remite algún conocido."

El mensaje sospechoso

"Estimada Marta

Hemos intentado entregar un paquete en la dirección indicada el día 15/07/2021 pero no ha sido posible. Acceda al siguiente enlace para revisar el punto de recogida de su paquete antes de 24h.

http://Y5u / Correos entrega /"

¿Qué hace Marta ante esta situación?

En cuanto Marta se percata de la dirección del enlace web, le parece muy sospechosa y no accede. Como no sabe quién es el remitente y tampoco esperaba ningún paquete,

cree que está siendo víctima de un engaño y siente que corre el peligro de acceder a una página maliciosa y descargarse un virus al teléfono para robar sus datos personales.

Así que decide **eliminar el mensaje SMS.**

Recuerda

Si recibes un SMS o mensajes extraños:

- No los abras
- No accedas a los enlaces o archivos.
- No descargues los archivos adjuntos.
- No los remitas a otros contactos.
- Elimínalos.

Estrategias para evitar el smishing

Si te piden datos, desconfía
Se debe desconfiar de cualquier requerimiento de datos personales, particularmente si se hace con urgencia. La mayor parte de los requerimientos pueden estar relacionados con envíos desde el extranjero, cambios en la entidad bancaria o cambios en la facturación de la línea de teléfono.

Revisa el número desde el que se realiza la llamada
Si la compañía de telefonía se pone en contacto, **lo usual es que lo haga desde el número habitual de atención al cliente.** Aun así, se debe desconfiar de un número que no esté dentro de la página oficial de la compañía, aunque al introducirlo en un buscador parezca asociado a la misma: cualquier persona puede haber editado una página web diciendo que ese número pertenece a la compañía. **Si es necesario realizar una comprobación, siempre ha de hacerse a través de los cauces ya conocidos (página web o teléfono de servicio al cliente).**

Examina la redacción del mensaje
Este tipo de mensajes **no suelen estar personalizados** y, además, **suelen tener una redacción propia de un traductor automático o, incluso, faltas de ortografía.** Las empresas grandes, en general, suelen cuidar mucho sus comunicaciones masivas; no sería propio que enviaran mensajes así.

No accedas a los enlaces de descarga
Si en el mensaje aparece un enlace de descarga se debe evitar pulsar sobre el mismo. En la mayoría de las ocasiones descargará un software malicioso.

¿Qué hacer si se es víctima de smishing?

- **Desconecta el móvil de Internet** y **cambia las contraseñas** de todos los servicios que creas que puedan haberse visto afectados desde otro dispositivo.
- Si piensas que tus claves bancarias han sido expuestas, es importante **dar aviso de inmediato al banco para informar de la situación y que bloqueen toda**

actividad que la persona ciberdelincuente pueda realizar con tu cuenta bancaria.

- **Elimina las aplicaciones infectadas**, si conoces cuáles son o realiza una restauración de fábrica para tener mayor tranquilidad. Previamente, es recomendable **tomar capturas para poder presentar una denuncia.**

4. CIERRE

4.1 Resumen

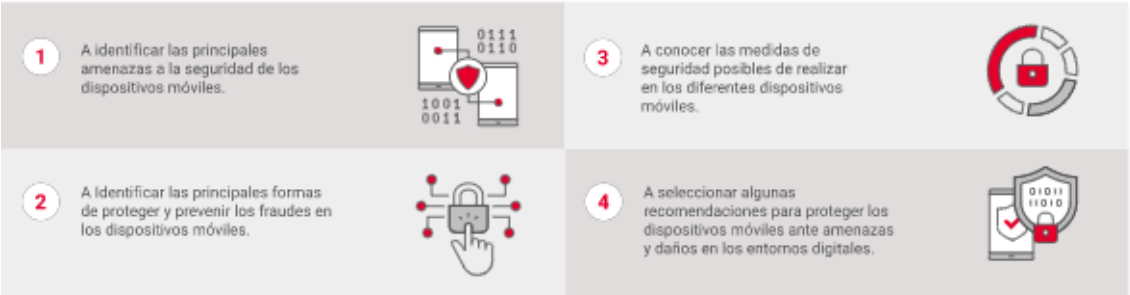
A lo largo de esta unidad didáctica Marta ha podido **identificar los riesgos que puede tener al trabajar con tanta información importante guardada en su móvil**. **Ha conocido las distintas medidas de seguridad y protección de sus datos** y ha logrado **seleccionar formas de proteger la información ante posibles daños de su dispositivo móvil**.

Hoy ha comenzado la ruta de aprendizaje para tener buenos hábitos de prevención en el uso de estos medios de comunicación, ya que comprende que es vital proteger su información.

¿Y qué has aprendido a hacer?

Acción Formativa 4. Seguridad en la red.

UNIDAD DIDÁCTICA 1. SEGURIDAD EN TERMINALES MÓVILES: CONFIGURACIÓN Y COPIAS DE SEGURIDAD



Una vez que has reflexionado y aprendido sobre los diferentes tipos de amenazas a las que te puedes enfrentar con tus dispositivos móviles y cómo puedes prevenir estos riesgos, en la siguiente Unidad Didáctica podrás ayudar a Marta a proteger sus claves, el robo de datos y así trabajar de forma segura en la red.

4.2 Referencias bibliográficas

A continuación, puedes ver la relación de recursos (artículos, estudios, investigaciones, páginas web...) que se han consultado y citado para elaborar el contenido de esta Unidad Didáctica:

- BBVA. (2020). Alerta de malware en dispositivos Android que suplanta la app de BBVA. Recuperado de: <https://www.bbva.es/finanzas-vistazo/ciberseguridad/ultima-hora/alerta-de-malware-en-dispositivos-android-que-suplanta-la-app-de-bbva.html> [09/02/2022].
- Comisión Europea. (2021). La Comisión refuerza la ciberseguridad de los dispositivos y productos inalámbricos. Recuperado de: <https://ec.europa.eu/commission/presscorner/detail/es/IP_21_5634> [09/02/2022].
- Diccionario panhispánico de dudas. (2005). Copia de seguridad. Real Academia Española. Recuperado de: <https://www.rae.es/dpd/copia%20de%20seguridad> [09/02/2022].
- Ibercaja. (2021) ¡No piques! ¡No pinches! Identifica rápidamente un ataque de phishing. Recuperado de: https://www.ibercaja.es/particulares/blog/consejos-utiles/phishing/ [09/02/2022].
- Instituto Nacional de Ciberseguridad. (2019). Cómo prevenir incidentes en los que intervienen dispositivos móviles. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles [09/02/2022].
- Instituto Nacional de Ciberseguridad. (2015). La importancia de las copias de seguridad de tus datos. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/importancia-copias-seguridad [09/02/2022].
- Instituto Nacional de Ciberseguridad. (2015). Decálogo de medidas de seguridad en el correo electrónico. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-correo-electronico [09/02/2022].
- El periodico. (2020). «O pagas 10.000€ o te enviamos un vídeo cortándole un dedo a tu hija». Recuperado de: https://www.elperiodico.com/es/sociedad/20200111/secuestro-expres-virtual-policia-nacional-7802262 [09/02/2022].
- Emprender, innovar, Trinufar. (2020). Emotet, el troyano más activo: afecta al 17% de las empresas españolas. Recuperado de: https://www.ticpymes.es/tecnologia/noticias/1121958049504/emotet-troyano-mas-activo-afecta-al-17-de-empresas-espanolas.1.html [09/02/2022].
- Oficina de seguridad del internauta. (2018). Detectando fraudes - Análisis de una web de venta falsa. Recuperado de: https://www.osi.es/es/actualidad/blog/2018/08/08/detectando-fraudes-analisis-de-una-web-de-venta-falsa [09/02/2022].
- Oficina de seguridad del internauta. (2022). Conoce la nueva directiva para reforzar la ciberseguridad de los dispositivos inalámbricos. Ciberseguridad.. Recuperado de: https://www.osi.es/es/actualidad/blog/2022/02/04/conoce-la-nueva-directiva-para-reforzar-la-ciberseguridad-de-los [09/02/2022].
- Oficina de seguridad del internauta. (2018). Smartphones y tabletas. Recuperado de: https://www.osi.es/es/smartphone-y-tablet [09/02/2022].
- Soporte de Apple. Cómo restablecer los ajustes de fábrica del iPhone, iPad o iPod touch. Recuperado de: <https://support.apple.com/es-es/HT201274> [09/02/2022].

- Soporte de Google. Encontrar y bloquear un dispositivo Android perdido o borrar sus datos. Recuperado de: <https://support.google.com/android/answer/6160491?hl=es> [09/02/2022].