Fundación Telefónica

ANDROID

04 Ciberseguridad básica

Nombre:

Lo primero, gracias por acudir a nuestro taller de formación. Esperamos que te haya sido útil, además de pasar un buen rato.

Con esta breve guía **queremos que tengas en casa temas explicados, cosas aprendidas** y alguna más que quizás se han quedado en el tintero.

A lo largo de las páginas encontrarás 5 bloques temáticos que te resultarán familiares:

1. Contraseñas
2. Protección de los dispositivos
3. Actualizaciones
4. Identificación de estafas
5. Fake news

Esperamos que te sirva de apoyo.

CONTRASEÑAS

Reflexiona sobre las siguientes cuestiones:

¿Qué riesgos crees que tenemos usando Internet?

¿Cómo crees que podemos protegernos de las amenazas de Internet?

¿Sabes identificar una contraseña segura?

1.1. Introducción

Aunque suponga un reto, el uso de las nuevas tecnologías e Internet es un gran avance que nos facilita realizar diversas actividades como encontrar información o comunicarnos. Debemos ser conscientes de que el uso de Internet también trae nuevas amenazas o situaciones que, en mayor o menor medida, implican un riesgos. Lo importante es concienciarnos y aprender.

Así, **deberás proteger tus dispositivos, navegar de forma segura a través de la Red e identificar los posibles riesgos**.

Los temas sobre los que debes reflexionar son:

- Accedemos y navegamos por Internet a través de dispositivos, por lo que debemos aprender a navegar con seguridad.

- En nuestro teléfono podemos llegar a almacenamos mucha información personal (teléfonos, direcciones, nombres, fotografías, mensajes, etc.) por lo que debemos tener cuidado y conocer quién puede acceder a ella.

1.1. Introducción

Temas que debes tener presentes:

Accedemos y navegamos por Internet a través de dispositivos, por lo que debemos aprender a navegar con seguridad.

En nuestro teléfono podemos llegar a almacenar mucha información personal (teléfonos, direcciones, nombres, fotografías, mensajes, etc.) por lo que debemos tener cuidado y conocer quién puede acceder a ella.

1.2. Contraseñas

"Una contraseña o *password* es una serie secreta de letras, números y signos para acceder a un servicio de Internet".

Casi seguro que has oído hablar de las contraseñas y utilizas alguna. ¿Usas la misma para todo? ¿Las tienes escritas en un papel?

Vamos a ver qué es esto de las contraseñas y cómo podemos hacer para que sean seguras y además no se te olviden.

Tus contraseñas no deberías compartirlas con nadie, son secretas.

1.3. Contraseñas más seguras

Fundación Telefónica

Contraseñas más seguras

Mínimos a tener en cuenta para que tu contraseña sea lo más robusta posible:

- Debe tener entre **8 y 12 caracteres.**
- Deberá incluir al menos **una letra en mayúscula.**
- Incorporar un **carácter especial.**

Ejemplo:

1. Pensar una palabra larga (la longitud mínima recomendada es de 10 caracteres) o grupo de dos o tres palabras. → RECONECTADOS
2. Alternar mayúsculas y minúsculas. → ReCoNecTaDos
3. Intercambiar algunas letras por cifras. (e=3 / i=1) → R3CoN3cTaDos
4. Añadir un carácter especial. (Espacio=_) → R3CoN3c_TaDos
5. Personalizar la clave para cada servicio. → R3CoN3c_TaDos_luz / R3CoN3c_TaDos_telefono

Ahora tú:

1. Piensa una frase. →
2. Une las palabras y alterna mayúsculas y minúsculas. →
3. Intercambia algunas letras por cifras. →
4. Añade un carácter especial. →

PROTECCIÓN DE LOS DISPOSITIVOS

2.2. Bloqueo de pantalla

Bloquear la pantalla de nuestro teléfono permite que podamos controlar el acceso de otras personas y proteger nuestra información personal. Cuando utilizamos nuestro móvil almacenamos información, fotografías, correos electrónicos, números de teléfono e incluso direcciones postales. Además, esta función permite que el teclado y la pantalla se apaguen mientras no estamos usándolo y evitar que se realicen llamadas o se pulse alguno de los botones externos del teléfono.

Los sistemas de bloqueo son como las llaves de la caja fuerte, con ellos conseguiremos poner muy difícil el acceso a nuestro teléfono.

Existen distintos tipos de bloqueo:

- PIN
- Patrón
- Huella dactilar
- Reconocimiento facial

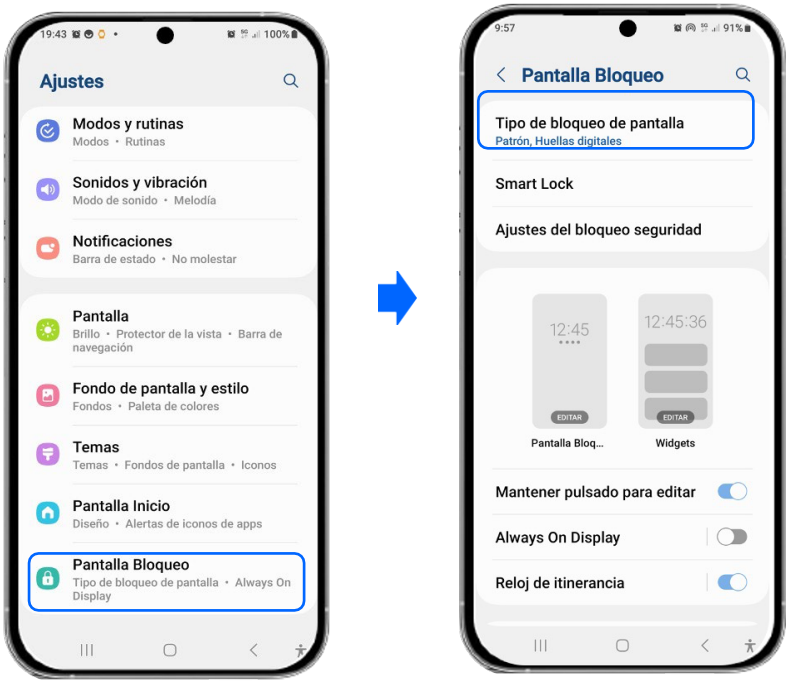
2.2. Bloqueo de pantalla

Hay que introducir un código de habitualmente 4-6 números. No tiene por qué ser el número PIN de acceso a tu teléfono.

Es un sistema de trazado de dibujo con el dedo uniendo una serie de nueve puntos

Pulsa en el icono de ajustes:

Sigue estos pasos:



ACTUALIZACIONES

3. Actualizaciones

Si los frenos de la bicicleta no funcionan, hay que arreglarlos para poder usarla.
Las actualizaciones ayudan a que los teléfonos móviles funcionen mejor.

> "Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad". (INCIBE).

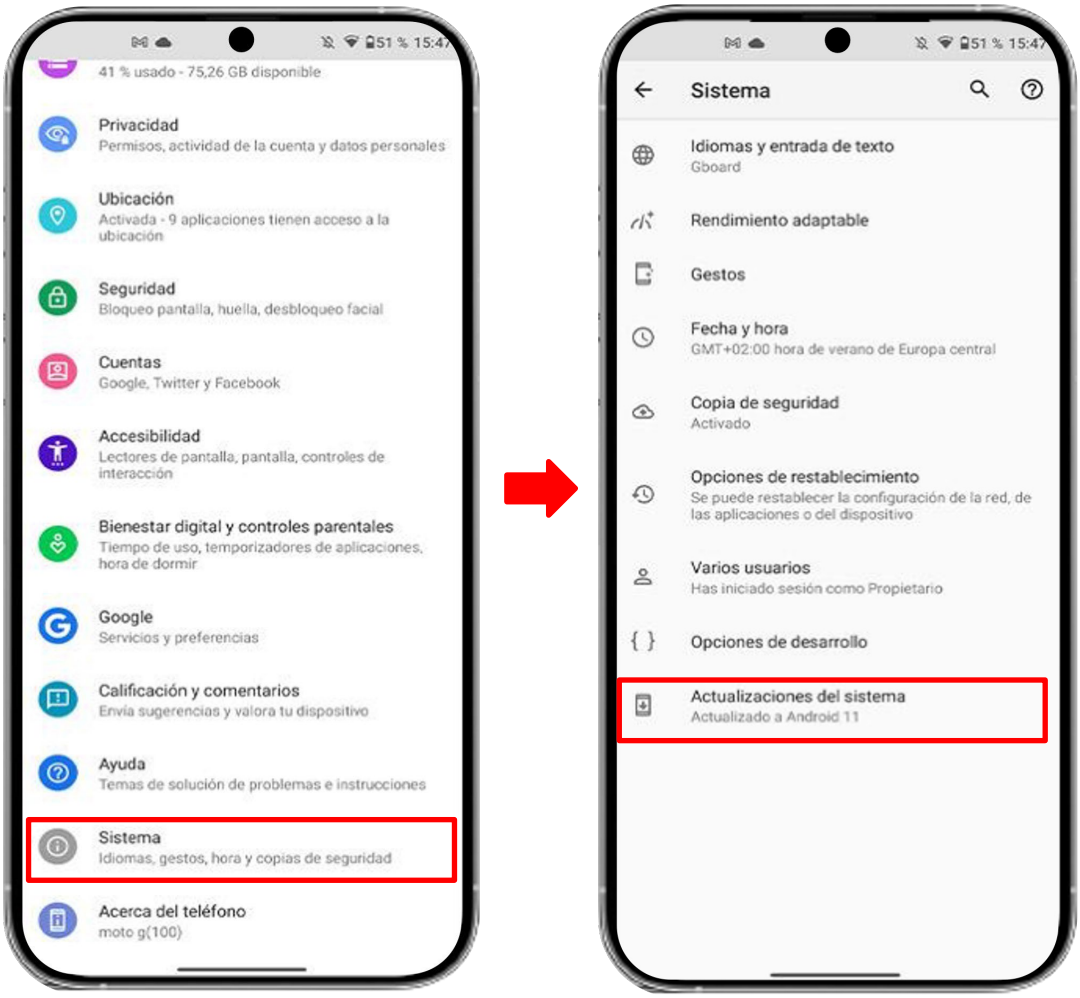
- Elige la actualización automática si está disponible.
- Instala las actualizaciones lo antes posible.
- Instala siempre desde la tienda de aplicaciones oficial, Play Store.

Actualización del sistema operativo - Android

Para este tipo de actualización deberás estar conectado a una red wifi de confianza, además de tener el teléfono enchufado al cargador.

Pasos que debes seguir:

- Ajustes >
- Sistema >
- Ajustes Avanzados >
- Actualizaciones del sistema >
- Actualizar >

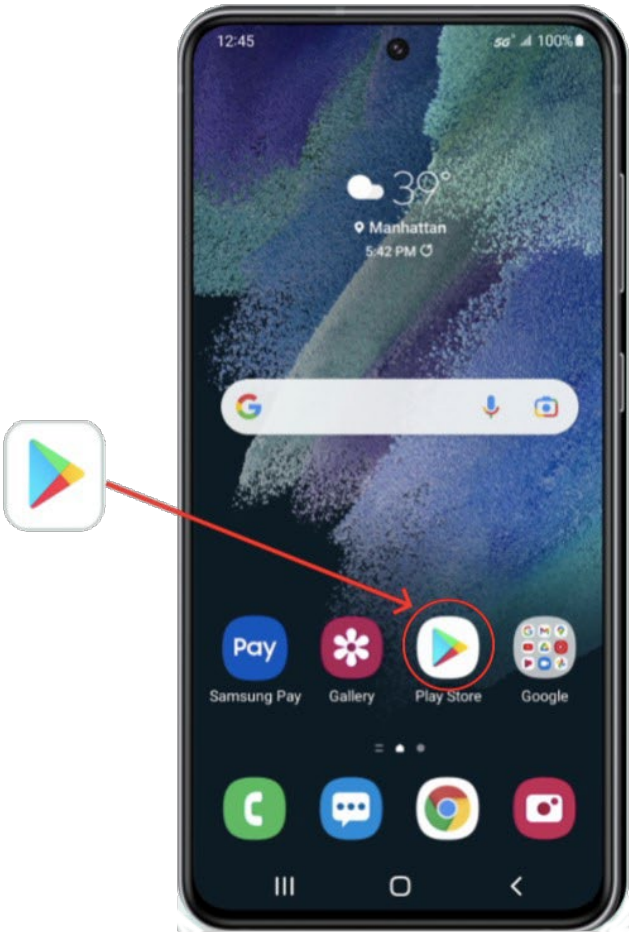


Actualización del sistema operativo - Android

Las actualizaciones también se hacen para las aplicaciones, ya sea por cuestiones de seguridad o porque incluyen una nueva funcionalidad.

Pasos que debes seguir:

- Entrar en Play Store >
- Buscar barra de búsqueda y la lupa >
- Escribir el nombre de la aplicación a actualizar >
- Hacer clic en "Actualizar">



Fundación Telefónica

IDENTIFICACIÓN DE ESTAFAS

4.1. Introducción

La tecnología puede utilizarse con **fines inadecuados.**

Cada vez es más frecuente recibir mensajes a través de correo electrónico y/o SMS **con el fin de engañarnos**, pero también a través de llamadas telefónicas.

En caso de sospechar de un fraude nunca se deben seguir las indicaciones, ninguna entidad de confianza te va a solicitar datos personales, números de cuenta o claves de acceso.

4.2. Tipos de estafas

Aprende a reconocer los distintos tipos de estafas:

Phishing

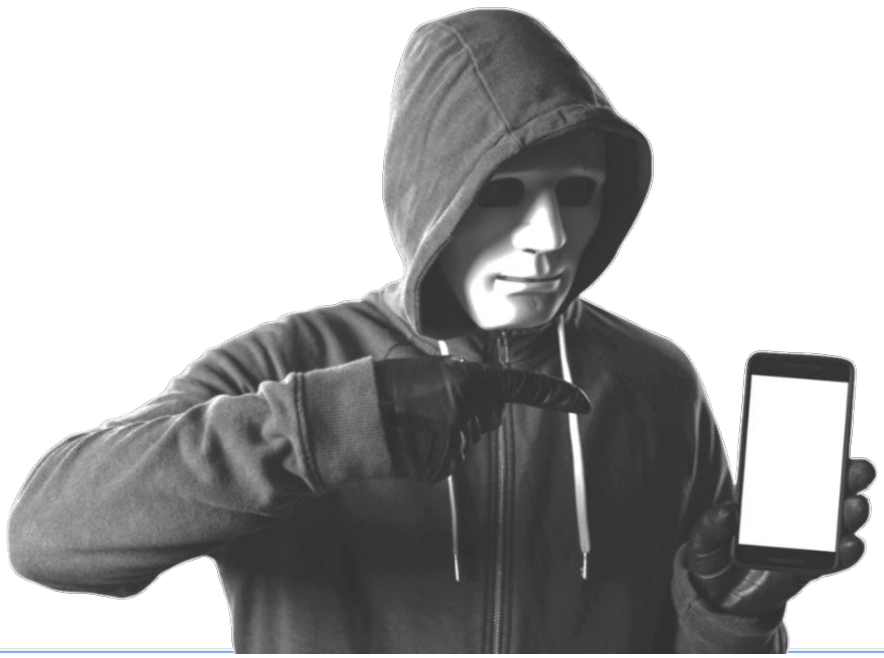
Morder el anzuelo, se trata de envíos al **correo electrónico** simulando ser una entidad legítima, por ejemplo un banco, la compañía de la luz, Seguridad Social. Su finalidad es conseguir la información personal y bancaria que puedan.

Vishing

Es un fraude que se suele llevar a cabo **vía telefónica**. Un supuesto operador/a se identifica como empleado/a de una entidad de confianza, un banco, la administración pública, compañía de telecomunicaciones... Además de querer conseguir datos personales, a veces, también quieren coger el control del dispositivo.

Smishing

En esta ocasión envían el fraude a través de **SMS**, de nuevo simulando ser una entidad de confianza, con el objetivo de robar información privada o realizar un cargo económico. Es muy común que el mensaje contenga un número para llamar (de tarificación especial) o un enlace de internet.



4.3. Cómo detectar una estafa

Cómo detectar una estafa:

1	Comprueba el remitente, en caso de aparecer un número desconocido o un correo electrónico extraño, lo más probable es que sea un fraude.
2	Analiza el apartado de "asunto" del correo electrónico, suelen ser llamativos.
3	Sé crítico con el objetivo del mensaje, qué es lo que quieren. En muchas ocasiones suelen solicitar una acción rápida, acotada en el tiempo.
4	Busca errores ortográficos y gramaticales. La explicación es porque están escritos a través de un traductor automático.
5	Asegúrate que lleva el certificado de seguridad https://o un candado pasando el cursor por encima o manteniendo el dedo pulsado.
6	Si hay archivo adjunto, verifica el nombre que tiene asociado.

FAKE NEWS

5. Fake news

Cada vez es más frecuente escuchar el término fake new, noticia falsa o bulo, todos los términos son correctos además de hacer referencia a lo mismo.

Las fake news se propagan de manera fácil a través de la Red, tienen como fin desinformar, engañas y manipular.

Uno de los canales más utilizado para su difusión es WhatsApp.

Antes de reenviar una noticia deberás tener claro que no es falsa, te damos las pautas de cómo saberlo.

Cómo identificar fake news

1. Busca y **contrasta la fuente.** Puedes buscar la misma noticia en un buscador para ver si sale en medios fiables.

2. Revisa el enlace y asegúrate que lleva el certificado de seguridad https:// o un candado.

3. **Los titulares suelen ser muy llamativos**, por ejemplo: "Encuentran una vacuna contra el cáncer".

4. Aplica el sentido común.

5. Analiza si es una broma, a veces se busca ironizar sobre una noticia.

Notas

Notas


Fundación
Telefónica