Programa universitario 50 plus José Saramago

MANUAL BÁSICO PARA APRENDER A MANEJAR TELÉFONOS MÓVILES.

ESTA GUIA BÁSICA ESTA PREPARADA PARA FACILITAR LA COMUNICACIÓN ENTRE TODOS Y PODER ESTAR INFORMADOS A TRAVES DEL MÓVIL

AUTORES: Marino Sanz Navarro
Raquel Cervigón Abad

ESPERAMOS QUE OS SEA DE UTILIDAD

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES FECYT INNOVACIÓN
UCLM
MUSEO DE LAS CIENCIAS DE CASTILLA-LA MANCHA
CULTURA SOSTENIBLE
SCIENCLM

Programa universitario 50 plus José Saramago

INDICE DE MATERIAS

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES FECYT INNOVACIÓN

UCLM

MUSEO DE LAS CIENCIAS DE CASTILLA-LA MANCHA

CULTURA SOSTENIBLE

SCIENCLM

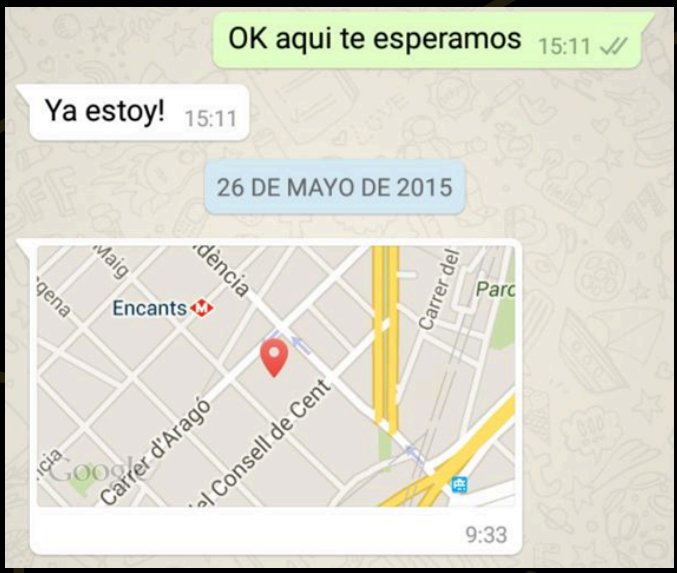
Programa universitario 50 plus José Saramago

INDICE DE MATERIAS

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT INNOVACIÓN · UCLM · MUSEO DE LAS CIENCIAS DE CASTILLA-LA MANCHA · CULTURA SOSTENIBLE · SCIENC LM

Programa universitario 50 plus José Saramago

DETALLE 1.0
CÓMO ENVIAR UNA UBICACIÓN POR WHATSAPP, PARA ANDROID Y IPHONE



Los **teléfonos móviles** cada vez nos ofrecen alternativas más inteligentes para facilitarnos la vida, y sin duda uno de los mejores adelantos es la opción de **GPS** que viene incorporada en estos dispositivos y que nos permite llegar a donde queramos de forma rápida y sin consultar a terceros.

Y para hacerlo aún más fácil es posible **enviar nuestra ubicación** a un contacto para que, con la ayuda de su GPS, llegue a donde estamos. ¿Quieres hacerlo peor no sabes cómo? En unComo.com te explicamos **cómo enviar una ubicación por WhatsApp** en Android y iPhone.

Pasos a seguir:

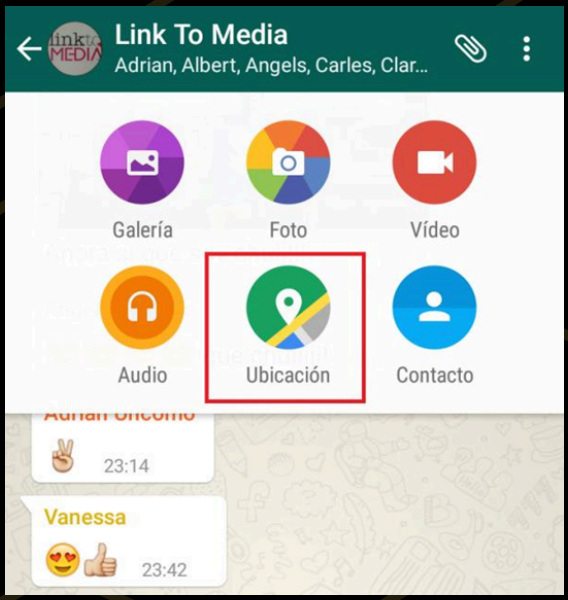
Enviar una ubicación por el móvil es la forma más rápida que tenemos para explicarle a otro contacto dónde estamos de manera que pueda llegar de forma directa. Lo mejor es que hacerlo, tanto en iPhone como en Android, es muy fácil.

Lo primero que debes hacer es **activar tu ubicación** para que el dispositivo pueda detectarla. Si intentas enviar esta información a otro contacto sin tener el GPS activado el sistema te indicará que debes encenderlo para que los datos puedan ser precisos y enviarse correctamente.

Comencemos por **Android**. Una vez que has activado la ubicación debes entrar a WhatsApp y seleccionar el contacto o grupo al que deseas enviar la ubicación. Dentro de chat presiona el **icono de clip** que se encuentra en la parte superior de la conversación.

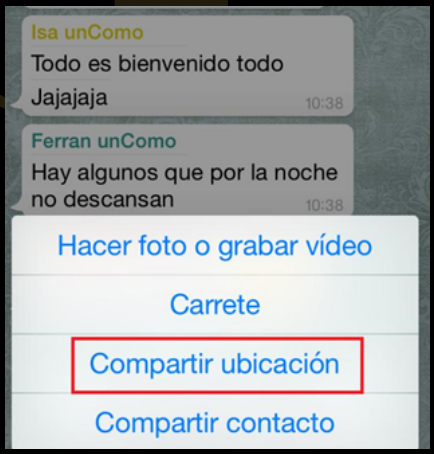
Allí encontrarás varias alternativas para compartir con ese contacto o grupo, debes elegir la opción de **Ubicación**. Al tener el GPS activado el sistema detectará dónde te encuentras y enviará la dirección a la persona elegida de forma simple y rápida. Además, es posible enviar tu ubicación actual o elegir entre distintos puntos de referencia cercanos a la zona donde te encuentras como tiendas, restaurantes, etc.

Tu contacto, al recibir la ubicación, simplemente deberá clicar sobre ella para ir a su mapa y ver dónde te encuentras.



En el caso de iPhone es igualmente sencillo **enviar tu ubicación por WhatsApp**. Simplemente deberás abrir la aplicación y elegir el contacto o grupo al que deseas enviar la dirección, luego presiona sobre el icono de la flecha que se encuentra ubicado en la parte inferior izquierda.

Se desplegará un menú de opciones, deberás elegir **Compartir ubicación**. Recuerda que para hacerlo deberás tener el GPS activado, de lo contrario no se podrá enviar en punto en el que te encuentras.



Programa universitario 50 plus José Saramago

DETALLE 1.0
CÓMO ENVIAR LA UBICACIÓN EN TIEMPO REAL DESDE TU MÓVIL

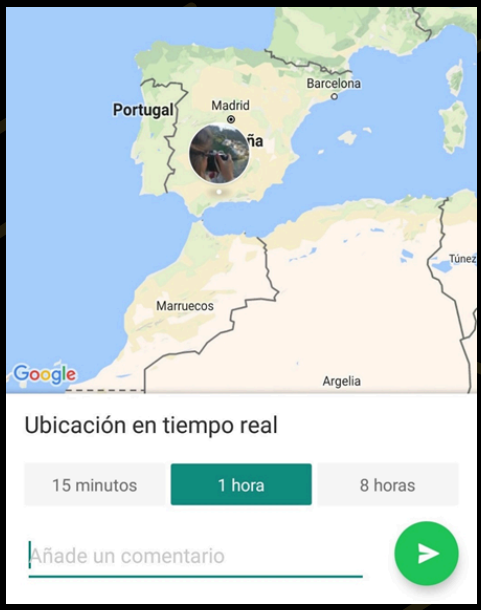
La ubicación en tiempo real es muy útil en muchos casos, pese a la controversia. Ya te dimos, hace tiempo, muchas razones por las que era una buena idea utilizar esta tecnología. Puedes usar la ubicación en tiempo real desde distintas aplicaciones en tu teléfono móvil y con quien tú quieras.

Te explicamos **cómo enviar la ubicación en tiempo real** a tu madre, tu pareja, tu primo o a quien tú quieras desde las distintas aplicaciones disponibles. No hará falta una aplicación concreta, sino que hay muchas opciones para usarla.

Desde WhatsApp

WhatsApp incorpora desde hace tiempo la ubicación en tiempo real. Permite que envíes la ubicación en cualquier chat que tengas abierto a cualquier persona con la que hables desde la aplicación. La persona a la que se la envíes verá durante el tiempo que tú quieras dónde estás (siempre y cuando tengas la ubicación activada en el móvil y no dejes de compartirla) para saber cuándo llegas o para saber si estás bien. Podrás enviarla **durante 15 minutos, 1 hora o durante ocho horas**.

Enviar la ubicación en WhatsApp es muy sencillo. Solo **pulsa en el clip** que aparece en el lateral del cuadro de texto del chat. Se abrirá, como ya sabes, un desplegable con opciones para enviar: documento, cámara, galería, audio, ubicación y contacto. Ve a Ubicación. Una vez allí, podrás elegir entre enviar Ubicación en tiempo real o "**Enviar ubicación actual**". Apuesta por la primera opción, elige el tiempo que quieres compartirlo y ya podrán seguirte.



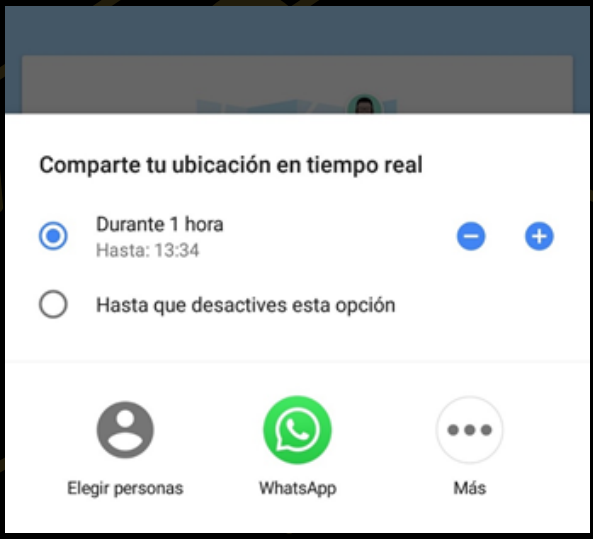
Desde Google Mapa (Maps)

Google Maps también permite que compartas la ubicación en tiempo real a través de un enlace si quieres hacerlo en cualquier otra aplicación que no sea WhatsApp. Podrás usarlo en Facebook Messenger, enviarlo por correo electrónico, por mensaje privado de Twitter...

Programa universitario 50 plus José Saramago

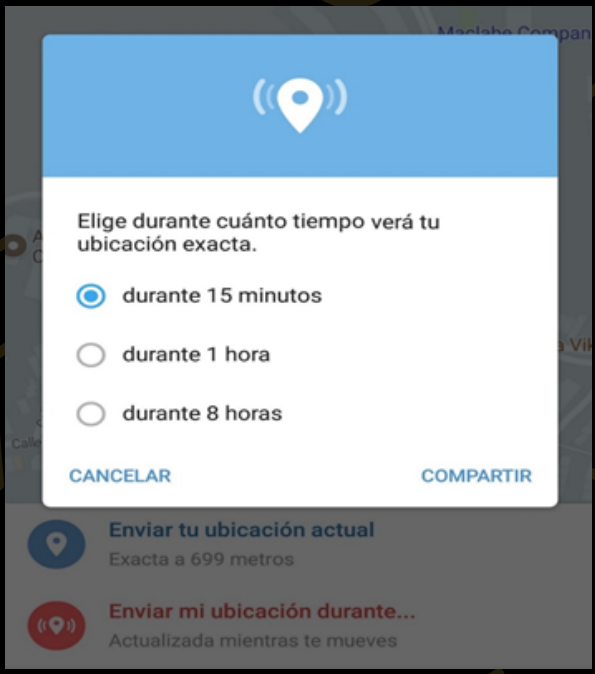
Para ello abre Google Maps en tu teléfono móvil, pulsa en las tres rayas de la parte de la izquierda para abrir el menú y busca la opción **“Compartir ubicación”**. Se aparecerá un menú en el que podrás elegir cuántas horas compartir la ubicación (o hasta qué hora) y elegir a través de qué aplicación compartirla. Podrás hacerlo por Gmail, Mensajes de Android, mensaje privado de Instagram, de Twitter... Envía a quien quieras y podrán

Esta opción es más completa que la de WhatsApp ya que podrás elegir dónde compartirla y cuánto tiempo exacto mientras que en WhatsApp solo podrás optar por usuarios que tengan la app y entre tres tiempos establecidos.



Desde Telegram

Desde Telegram también puedes enviar la ubicación en tiempo real y es similar a WhatsApp. Basta con que pulses sobre el menú de adjuntar > ubicación > enviar mi ubicación durante... Podrás elegir, al igual que en WhatsApp, enviar durante 15 minutos o 1 hora u 8 horas.



Aplicaciones:

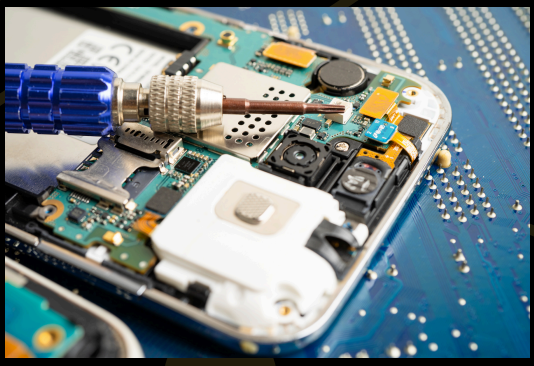
WhatsApp
Twitter
Facebook
LinkedIn

TODAS ESTAS APLICACIONES (Apps), tienen **la misma forma de enviar la ubicación**.

DETALLE 1.2
APLICACIONES EN SEGUNDO PLANO

Seguro que alguna vez has oído hablar o has visto que tu móvil está ejecutando **aplicaciones en segundo plano** y no le has dado la importancia suficiente. ¿Sabías que es un aspecto que **afecta al rendimiento del dispositivo y al consumo de batería**?

Una de las principales consecuencias que esto conlleva es que tu dispositivo consumirá más recursos de lo habitual. No obstante, no tiene por qué ser necesariamente algo negativo, ya que si nos aventuramos a **conocer cómo funciona la gestión de la RAM de un móvil**, podemos encontrar una serie de beneficios al respecto.



¿QUÉ ES Y CÓMO FUNCIONA LA MEMORIA RAM?

La memoria RAM de los teléfonos móviles está ideada para almacenar información temporal a la que se accede de manera habitual, en este caso la de las aplicaciones, y tiene como objetivo que el usuario no tenga que cargarla al abrirla de nuevo. Es decir que, al abandonar una aplicación, ésta estará preparada para no volver a iniciarse desde cero la siguiente vez que queramos acceder a ella.

¿Cómo cerrar una aplicación en segundo plano?

Cerrar aplicaciones en segundo plano es una tarea realmente fácil. Tan solo tienes que dirigirte a la **sección "Aplicaciones" dentro de "Ajustes"**, buscar cuál es la app en cuestión que quieres que deje de utilizar recursos de tu teléfono móvil y **seleccionar "Forzar detención"**.

Un **truco** para descubrir cuáles son las aplicaciones que más consumen es ir a la **sección de "Batería"**, donde tu móvil te mostrará **qué porcentaje ha gastado cada una de ellas y durante cuánto tiempo de uso**.

Este comportamiento se traduce en que **el móvil haga un uso más intensivo de su procesador**, lo que conlleva un **gasto mayor de batería** y, consecuentemente, que la salud de ésta se deteriore con mayor rapidez de lo habitual.

Otro truco que puedes aplicar es el de **limitar el uso de datos en segundo plano**. Para ello ve a la **sección de "Aplicaciones"** dentro de "Ajustes", **accede a "Uso de datos" y desactiva la casilla que dice "Datos en segundo plano"**.

Programa universitario 50 plus José Saramago

¿Cómo puedo mejorar el rendimiento de mi móvil?
Además de todo lo mencionado sobre las aplicaciones en segundo plano, aquí tienes otros **puntos complementarios para que el rendimiento de tu móvil y la salud de su batería sean los adecuados:**

·**Instala solamente las aplicaciones que vayas a usar frecuentemente**. Solo tú sabes cuáles son las que vas a necesitar en el día a día, por lo que detecta aquellas que tengas en desuso y desinstálalas para ahorrarte un posible consumo en segundo plano innecesario.

·**Borra el caché de las aplicaciones**. Con este sencillo hábito podrás liberar espacio de tu teléfono móvil y que tenga un funcionamiento algo más fluido. También puedes hacerlo dentro del navegador que uses por defecto, ya que tendrá acumulados datos de la infinidad de búsquedas que habrás hecho. **Siempre viene bien una limpieza periódica.**

Como último recurso, restablece el móvil. En ocasiones, tener unos buenos hábitos de carga del móvil, tenerlo actualizado o no almacenar contenido innecesario no es suficiente para que un smartphone funcione como debe. Estos dispositivos se van quedando obsoletos con el paso del tiempo y puede darse el caso de que **la solución para limpiarlo del todo sea hacerle un reseteo y dejarlo "de fábrica"**.

Programa universitario 50 plus José Saramago

DETALLE 1.3
APLICACIONES DUALES

Las **aplicaciones duales** son aquellas que se pueden duplicar de tal forma que se comporten como dos aplicaciones totalmente independientes la una de la otra.

Las aplicaciones duales son aquellas que nos permiten tener **dos versiones diferentes de la misma aplicación**, ya sea de Whatsapp, o de algún juego en el que tengamos dos cuentas, etc. Podemos disponer de dos aplicaciones iguales, con una cuenta diferente cada una.

Cómo crear aplicaciones duales

En Xiaomi

Crear aplicaciones duales desde un dispositivo Xiaomi es una tarea muy sencilla. La función también está disponible en Redmi, filial de la conocida Xiaomi.

Para duplicar aplicaciones en Xiaomi/Redmi se han de seguir los siguientes pasos:

- Acceder a los **Ajustes** del dispositivo móvil.
- Buscar el apartado de "**Aplicaciones**" y hacer clic sobre ella.
- Una vez dentro buscar la que dice "**Aplicaciones Duales**" y pulsar sobre ella.
- **Escoger ahora una app a clonar**, y aceptar los servicios de Google. Luego se creará una segunda aplicación con la que ejecutar esa segunda cuenta, ya sea una aplicación o bien un juego.

En Huawei

En dispositivos Huawei/Honor la creación de aplicaciones duales se llama "**App gemela**", viene deshabilitada por defecto en todos los modelos. En la última versión es posible al menos clonar tres, Facebook, Facebook Messenger y WhatsApp, cada una de ellas de manera limpia y empezando desde cero.

Para duplicar aplicaciones con App gemela en Huawei/Honor hay que realizar los siguientes pasos:

- Abrir **Ajustes** en el dispositivo Huawei/Honor.
- Una vez dentro acceder a **"Aplicaciones" o "Aplicaciones y notificaciones"** y busca "**App gemela**", pulsar sobre las apps permitidas.
- Al pulsar en la que se quiere clonar dirá "**Creando aplicación gemela**", se mostrará en el escritorio la segunda aplicación creada, y luego solo quedará pulsar sobre ella.

En Huawei existe una gran limitación, aunque para llegar a más aplicaciones lo mejor es instalar la herramienta **Paralell Space**, una app para tener aplicaciones multicuenta.

¡¡¡¡Como siempre indicaros que estas aplicaciones, si las bajáis para instalarlas en el teléfono, deben ser gratuitas y de proveedores conocidos, - aunque lleven anuncios, para su mantenimiento-, y si no es una necesidad imperante, mejor no bajarlas, la recomendación de una aplicación es para tener conocimiento de su existencia, puede haber otras que realicen las mismas acciones!!!!

Programa universitario 50 plus José Saramago

En OnePlus

OxygenOS de OnePlus tiene entre sus características el poder usar las aplicaciones duales gracias a "**Aplicaciones paralelas**", una de las tantas funciones disponibles en esta capa.
Todos los modelos de OnePlus tienen esta opción disponible, desde los primeros a los últimos, por ello es aconsejable tener actualizada la aplicación.

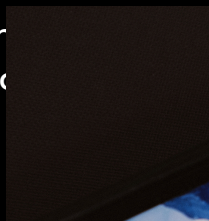
Para duplicar aplicaciones con cualquier dispositivo OnePlus hay que hacer lo siguiente:

- Acceder a los **Ajustes** del dispositivo OnePlus.
- Buscar entre las tantas utilidades "**Aplicaciones paralelas**" y haz clic sobre ella.
- En el listado se mostrará todas las aplicaciones que se pueden clonar, y **hay que elegir una de ellas**.
- Al igual que sucede con las demás, **se creará un nuevo icono de la aplicación que se haya decidido copiar**.

En Oppo

Oppo con ColorOS también deja lanzar aplicaciones duales. Se pueden clonar casi cualquiera de ellas, todo sin la necesidad de descargar Paralell Space.
De querer duplicar aplicaciones con ColorOS se debe de hacer lo siguiente en el teléfono Oppo:

- Abrir los **Ajustes** del teléfono.
- Buscar la opción **App Cloner** (Clonador de aplicaciones) y pinchar sobre ella.
- Ahora se mostrará el listado de las apps dispor clonar. Crea un icono de manera rápida en el esc teléfono para poder usarla desde cero.



En cualquier otro teléfono

De querer usar aplicaciones duales en cualquiera de los teléfonos existente todo pasa por usar **Parallel Space**, ya sea su versión estándar o de 64 bits. La última está pensada para rendir en aquellos dispositivos con un procesador más moderno, ya que los recursos van a ser superiores. Para ello hay que **descargar la aplicación de la Play Store e instalarla en el teléfono** para empezar a duplicar cualquier aplicación de las instaladas en el smartphone.

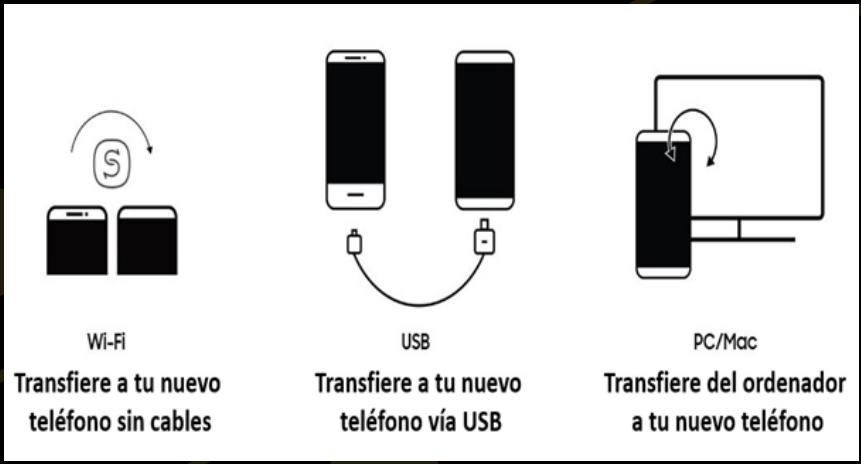
Para duplicar aplicaciones con Parallel Space se debe seguir el paso a paso siguiente:

- **Abrir Parallel Space**, todo ello después de haberla instalado.
- Se mostrará el listado completo de aplicaciones instaladas, y hay que **seleccionar aquella a clonar**.
- Hacer clic en "**Añadir en Parallel Space**".
- Después de añadirla creará una copia de aquella aplicación seleccionada, si es por ejemplo WhatsApp se verá una app al igual que la original. Hay que pulsar sobre ella y configurarla desde el principio. Para ello **se pedirá un nuevo número de teléfono, por lo que hay que asegurarse de tener una segunda SIM insertada en la ranura**.
- **Si es otra solamente hay que añadir el correo electrónico y la contraseña para acceder**, por ejemplo, si es una red social como Instagram, Facebook, Twitter, etc.

Entrar en la aplicación duplicada **no afectará en na primera**, la que se usa habitualmente con el número p segunda actuará como si se estuviera utilizado otro telé

Programa universitario 50 plus José Saramago

DETALLE 2.0
TRASFERIR DATOS DE UN VIEJO MÓVIL A UNO NUEVO



Hay **tres métodos sencillos** para transferir tus datos: a través de **Wi-Fi, usando un cable USB o mediante un PC o Mac**.

Puedes encontrar **Smart Switch** en tu teléfono accediendo a **Ajustes > Nube y cuentas > Smart Switch**.

Descargar e instalar Smart Switch (Atención al descargar)
1.- **Descarga la aplicación de Smart Switch desde Google Play Store o Samsung Galaxy Apps** tanto en el dispositivo nuevo como en el antiguo.

2.- **Inicia la app y acepta los términos** y condiciones en ambos dispositivos.

3.- Una vez instalada la aplicación, tus dispositivos están preparados para realizar la transferencia de datos.

- **Cómo transferir datos de un teléfono Android a tu Samsung Galaxy**
- **Cómo transferir tus datos mediante USB o Wi-FiClick to Expand**
- **Cómo transferir tus datos mediante un PC o MacClick to Expand**
- **Qué datos se pueden copiar con Smart Switch**

Para conocer qué tipos de contenidos puedes trasladar con Smart Switch a través de cada uno de los métodos disponibles consulta las siguientes tablas.

Puedes encontrar **Smart Switch** en tu teléfono accediendo a **Ajustes > Nube y cuentas > Smart Switch**.

Descargar e instalar Smart Switch (Atención al descargar)
1.- **Descarga la aplicación de Smart Switch desde Google Play Store o Samsung Galaxy Apps** tanto en el dispositivo nuevo como en el antiguo.

2.- **Inicia la app y acepta los términos** y condiciones en ambos dispositivos.

3.- Una vez instalada la aplicación, tus dispositivos están preparados para realizar la transferencia de datos.

Programa universitario 50 plus José Saramago

Preguntas relacionadas

Qué hacer si tu dispositivo no detecta una tarjeta SD
En primer lugar, apaga el teléfono para manipular la tarjeta SD.

Paso 1. Apaga el teléfono e inserta la herramienta de extracción en el pequeño agujero junto a la bandeja de la tarjeta SD para expulsar la bandeja.

Paso 2. Revisa si la tarjeta SD está dañada.

En tu dispositivo, toca Ajustes. Toca Mantenimiento del dispositivo Almacenamiento. Comprueba si se reconoce la tarjeta SD. Si en Ajustes no se detecta la tarjeta SD, quítala y vuelve a insertarla.

Si la tarjeta SD y el lector de tarjetas están limpios y la tarjeta SD aún no se puede detectar, debemos conectar la tarjeta SD a la computadora con otro lector de tarjeta para verificarlo. Si aún no puede detectar la tarjeta SD al final, es posible que su lector de tarjetas tenga un problema.

Para hacer que nuestro teléfono móvil vuelva a reconocer la tarjeta micro SD en Android, tendremos que darle formato, es decir, formatearla, desde el propio sistema.

Programa universitario 50 plus José Saramago

DETALLE 3.0
QUÉ HACER SI TE ROBAN O PIERDES TU MÓVIL

Los smartphones en la actualidad son pequeñas super máquinas con las que llevamos casi toda nuestra vida en el bolsillo del pantalón. Como si de un DNI se tratase, cada teléfono inteligente y tableta está identificado con una numeración única, que se llama IMEI. Este número es necesario conocerlo para poder identificar el dispositivo, y actuar en consecuencia si nos lo roban o lo perdemos. Para conocerlo, marca en tu móvil *#06#

1. Intentar encontrar nuestro móvil

En caso de que pierdas o te roben tu dispositivo Android puedes encontrarlo empleando otro dispositivo conectado y accediendo a esta página de Google. Si tu Android está asociado a esa misma cuenta y está conectado a internet, aparecerá en el mapa.

2. Bloquear el smartphone con PIN, patrón o contraseña de forma remota

Esta opción consiste en bloquear el smartphone con PIN, patrón o contraseña. Y si no tienes una opción de bloqueo puedes crearla en ese momento, a distancia. En la pantalla de bloqueo podrás incluir un mensaje y número de teléfono para que te devuelvan el dispositivo.

3. Borrar todo lo que haya en nuestro móvil de forma remota

Si no consigues dar con él, y guardas datos importantes en tu smartphone, lo último que puedes hacer es borrar la información de forma remota utilizando también la opción de "Encontrar mi dispositivo".

Programa universitario 50 plus José Saramago

DETALLE 3.0
QUÉ HACER SI TE ROBAN O PIERDES TU MÓVIL

Los smartphones en la actualidad son pequeñas super máquinas con las que llevamos casi toda nuestra vida en el bolsillo del pantalón. Como si de un DNI se tratase, cada teléfono inteligente y tableta está identificado con una numeración única, que se llama IMEI. Este número es necesario conocerlo para poder identificar el dispositivo, y actuar en consecuencia si nos lo roban o lo perdemos. Para conocerlo, marca en tu móvil *#06#

1. Intentar encontrar nuestro móvil

En caso de que pierdas o te roben tu dispositivo Android puedes encontrarlo empleando otro dispositivo conectado y accediendo a esta página de Google. Si tu Android está asociado a esa misma cuenta y está conectado a internet, aparecerá en el mapa.

2. Bloquear el smartphone con PIN, patrón o contraseña de forma remota

Esta opción consiste en bloquear el smartphone con PIN, patrón o contraseña. Y si no tienes una opción de bloqueo puedes crearla en ese momento, a distancia. En la pantalla de bloqueo podrás incluir un mensaje y número de teléfono para que te devuelvan el dispositivo.

3. Borrar todo lo que haya en nuestro móvil de forma remota

Si no consigues dar con él, y guardas datos importantes en tu smartphone, lo último que puedes hacer es borrar la información de forma remota utilizando también la opción de "Encontrar mi dispositivo".

Programa universitario 50 plus José Saramago

¿Qué hacer si nos roban o perdemos nuestro móvil iPhone?

Buscar el dispositivo en un mapa

Para encontrar tu dispositivo, inicia sesión en iCloud.com/find. O usa la app Buscar en otro dispositivo Apple de tu propiedad. Si el iPhone, el iPad o el iPod touch no aparece en la lista de dispositivos, Buscar no está activado. Pero aún puedes proteger tu cuenta, aunque Buscar no esté activado.

Marcar el dispositivo como perdido

Cuando marcas el dispositivo como perdido, lo bloqueas de forma remota con un código de acceso y mantienes tu información segura. También se desactiva Apple Pay en el dispositivo perdido. Puedes mostrar también un mensaje personalizado con tu información de contacto en el dispositivo perdido.

Encontrar el número de serie.

PRESENTAR RECLAMACION SI ESTAS ACOGIDO A “AppleCare+”

Borrar tu dispositivo de forma remota

Una vez borrado tu dispositivo no podrás rastrear su ubicación, así que asegúrate de que ya no necesitarás buscar el dispositivo. Si tienes AppleCare+ con robo y pérdida, no borres el iPhone hasta que se haya aprobado la reclamación.

Una vez borrado tu dispositivo no podrás rastrear su ubicación, así que asegúrate de que ya no necesitarás buscar el dispositivo. Si tienes AppleCare+ con robo y pérdida, no borres el iPhone hasta que se haya aprobado la reclamación.

Eliminar el dispositivo perdido de la cuenta

Si tienes AppleCare+ con robo y pérdida, no elimines el iPhone perdido hasta que se haya aprobado la reclamación. Ve a appleid.apple.com para eliminar el dispositivo perdido de la lista de dispositivos de confianza.

MUY IMPORTANTE

Presentar denuncia ante las autoridades aportando todos los detalles que tengamos, muchos de ellos antes citados. Si el dispositivo perdido es un iPhone o un iPad con datos móviles, informa al operador de telefonía móvil al respecto de igual forma si nuestro móvil es un Android. Solicita al operador que desactive la cuenta para evitar que se realicen llamadas, se envíen mensajes de texto y se consuman datos. Además, si el dispositivo está cubierto por un plan del operador de telefonía móvil, presenta una reclamación.

Programa universitario 50 plus José Saramago

Precaución, ante todo

Por último, recordaros que antes de llegar a una situación de pérdida o robo es mejor hacer uso de una serie de medidas de profilaxis que nos ahorrarán algún que otro lamento. Es importante no perder ojo del móvil en zonas concurridas y no dejarlo nunca a la vista (por ejemplo, en la mesa de un bar) pero sobre todo no olvidemos nunca tener activadas las herramientas de búsqueda que los fabricantes ponen a nuestra disposición.

Crear una cuenta de Gmail

Para registrarte en Gmail, tienes que crear una cuenta de Google. Puedes usar ese nombre de usuario y esa contraseña para iniciar sesión en Gmail y en otros productos de Google como YouTube, Google Play y Google Drive.

Registrarse para obtener una cuenta de Gmail

1. Ve a la dirección

https://support.google.com/mail/answer/56256?hl=es

1. Sigue los pasos que aparecen en la pantalla para configurar tu cuenta.
2. Utiliza la cuenta que acabas de crear para iniciar sesión en Gmail.

Programa universitario 50 plus José Saramago

OBSERVACIONES

El nombre de usuario que quiero no está disponible

No podrás tener una dirección de Gmail determinada si el nombre de usuario que has solicitado:

- Ya está en uso.
- Es muy similar a un nombre de usuario existente (por ejemplo, si ejemplo@gmail.com ya existe, no puedes usar ejemp1o@gmail.com).
- Es igual que un nombre de usuario que utilizó alguien en el pasado y luego eliminó.
- Está reservado por Google para evitar el spam o el uso inadecuado.

Alguien está suplantando mi identidad

Si sospechas que alguien ha creado una dirección de Gmail para intentar suplantar tu identidad, puedes hacer lo siguiente:

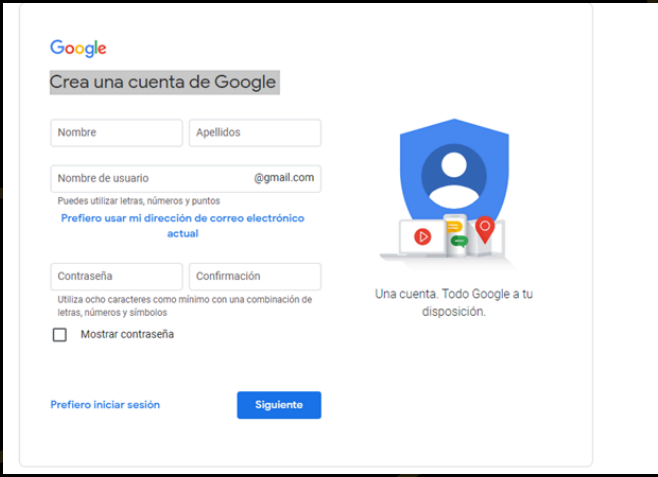
- Presentar una denuncia al Internet Crime Complaint Center (centro de denuncias de delitos en Internet).
- Ponerte en contacto con la oficina de protección al consumidor de tu zona.

Desafortunadamente, Gmail no puede participar en mediaciones con terceros implicados en una suplantación de identidad.

Programa universitario 50 plus José Saramago

DETALLE 4.0
CREAR UNA CUENTA EN GOOGLE

Estas pantallas que mostramos, que pueden ser cambiada por el proveedor Google, nos permiten conocer como nos van a pedir los datos para crear una cuneta de correo electrónico



Es importante tener al menos dos cuentas de e-mail para no comprometer la principal. Puedes tener una más personal, la que utilices para ponerte en contacto con amigos, familiares, estudios, cuando tengas que dar una dirección a alguna administración pública, etc. Por otro lado, puedes tener otra para cualquier cosa que pueda tener cierto riesgo.

Programa universitario 50 plus José Saramago

¿Qué entendemos por riesgo?

Por ejemplo, registrarte en una página o foro de Internet donde no sabes realmente si tus datos pueden estar en peligro o van a empezar a enviarte publicidad constantemente. El objetivo es mantener lo más limpio posible el correo principal. Así evitarás Spam, recibir publicidad constantemente o mensajes que realmente no te interesan.

Pero también debes tener en cuenta la seguridad. Cuanto más utilices una dirección de correo, más riesgos hay de que puedas sufrir algún ataque. Por ejemplo, podrías registrarte en alguna página de Internet y que en algún momento sufra alguna filtración. Eso va a poner en riesgo tus datos personales, como puede ser la cuenta de e-mail que has utilizado.

No significa necesariamente que puedan entrar en tu correo, sino que podrían simplemente incluirte en una lista de Spam o empezar a enviarte correos Phishing personalizados.
Por ello, cuidar tu dirección principal es importante y es buena idea utilizar al menos dos cuentas diferentes para no tener problemas.

Es importante tener al menos dos cuentas de e-mail para no comprometer la principal. Puedes tener una más personal, la que utilices para ponerte en contacto con amigos, familiares, estudios, cuando tengas que dar una dirección a alguna administración pública, etc. Por otro lado, puedes tener otra para cualquier cosa que pueda tener cierto riesgo.

Programa universitario 50 plus José Saramago

Google

Crea una cuenta de Google

Nombre | Apellidos

Introduce el nombre y los apellidos

Nombre de usuario @gmail.com

Elige una dirección de Gmail

Prefiero usar mi dirección de correo electrónico actual

Contraseña | Confirmación

Introducir una contraseña

☐ Mostrar contraseña

Prefiero iniciar sesión

Siguiente

Una cuenta. Todo Google a tu disposición.

Google

Te damos la bienvenida a Google

abcdedfgh894@gmail.com

Teléfono (opcional)

Google solo usará este número para mantener la seguridad de la cuenta. No lo mostrará a otros usuarios. Más tarde podrás elegir si quieres que se use con otros fines.

Dirección de correo electrónico de recuperación (o...

La usaremos para mantener tu cuenta protegida

Día | Mes | Año

Tu fecha de nacimiento

Género

Por qué pedimos esta información

Tu información personal es privada y está protegida

Eliminar tu cuenta de Google

Dirección del soporte de ce eliminación de cuenta en Google
https://support.google.com/mail/answer/32046?hl=es
Puedes eliminar tu cuenta de Google en cualquier momento. No obstante, si cambias de opinión, es posible que no puedas recuperarla.

Paso 1: Descubre qué ocurre al eliminar tu cuenta

- Perderás todos los datos y el contenido de la cuenta en cuestión, como correos electrónicos, archivos, calendarios y fotos.
- No podrás usar los servicios de Google en los que inicies sesión con esa cuenta, como Gmail, Drive, Calendar o Play.
- Perderás el acceso a las suscripciones y al contenido que hayas comprado con esa cuenta en YouTube o en Google Play, como aplicaciones, películas, juegos, música y programas de TV.

Si se ha pirateado tu cuenta

Antes de eliminar una cuenta hackeada o vulnerada, puedes consultar la página Revisión de Seguridad para obtener más información sobre las partes de la cuenta a las que se ha accedido sin tu permiso:
·Si guardas contraseñas en tu cuenta de Google, puedes averiguar si se ha accedido a ellas y si es necesario cambiarlas.
·Si guardas los contactos en tu cuenta de Google, sabrás si se han descargado y así podrás advertirles de que tengan cuidado con los mensajes sospechosos.
·Si usas Google Wallet para hacer transacciones, puedes comprobar si hay pagos no autorizados para disputarlos.
Importante: Una vez que se haya eliminado tu cuenta, ya no podrás utilizar la Revisión de Seguridad para examinar su actividad.

Paso 2: Revisa y descarga tu información

Antes de eliminar la cuenta:

- Revisa la información de tu cuenta. Obtén información sobre cómo descargar los datos que quieras conservar.
- Si usas tu dirección de Gmail en bancos online, redes sociales o aplicaciones, añade otra distinta a estos servicios.
- Actualiza la información de recuperación de la cuenta por si necesitas recuperar la cuenta más adelante.

Paso 3: Elimina la cuenta

Nota: Si tienes varias cuentas de Google, al eliminar una no se eliminarán las demás.

1. Ve a la sección Datos y privacidad de tu cuenta de Google.
2. Desplázate hasta "Tus datos y opciones de privacidad".
3. Selecciona Más opciones Eliminar tu cuenta de Google.
4. Sigue las instrucciones para eliminar tu cuenta.

Si no quieres eliminar tu cuenta de Google por completo, consulta cómo:

- Eliminar Gmail de tu cuenta.
- Quitar otros servicios de Google.
- Quitar aplicaciones con acceso a tu cuenta

Para quitar una cuenta de tu dispositivo sin eliminarla, sigue las instrucciones que se indican a continuación.

- Teléfono Pixel
- Dispositivo Nexus
- Otros dispositivos Android

Recuperar la cuenta

Si cambias de opinión o has eliminado tu cuenta accidentalmente, es posible que puedas recuperarla. Descubre cómo puedes recuperar tu cuenta.

Programa universitario 50 plus José Saramago

DETALLE 5.0
CONTRASEÑAS

Reglas a seguir

Por supuesto, habiendo destacado la falta de una guía eficaz, sería negligente terminar sin ofrecer alguna. La guía del NCSC sobre la elección y uso de contraseñas se enumeran y se explican brevemente a continuación:

- Utiliza una contraseña segura y distinta a la de tu su correo electrónico, ya que esta suele ser tu ruta para acceder a otras cuentas.
- Crea contraseñas seguras con tres palabras aleatorias; esto te dará contraseñas más seguras y memorables.
- Guarda tus contraseñas en tu navegador; esto evita que las olvides o las pierdas.
- Activa la autenticación de dos factores: esto agrega un elemento adicional de protección incluso si tu contraseña está comprometida.

Es útil complementar esto con recordatorios adicionales para no usar la misma contraseña en varias cuentas por temor a que la violación de una lleve a la violación de todas, no compartirlas con otras personas, porque entonces ya no es tu contraseña y no mantener un registro visible de las mismas.

Almacenarlas en un sitio protegido, como una herramienta de administración de contraseñas, está bien.

Es preocupante pensar que las contraseñas han existido durante décadas y todavía nos equivocamos. Y son solo un aspecto de la ciberseguridad que debemos utilizar correctamente.

Algunos consejos y buenas prácticas para tus contraseñas

- No utilices la misma clave para todo, utiliza una clave distinta para cada servicio.
- Cambia las contraseñas cada cierto tiempo.
- Habilita la autenticación en dos pasos si el servicio te lo permite. Así, te enviarán un mensaje al móvil para acceder a tu cuenta.
- No le digas a nadie tu contraseña, ni la escribas en un post-it.
- Cuanto mayor sea la longitud de tu clave, más segura será. Es recomendable que tenga al menos 8 caracteres de longitud. Lo ideal es que tenga más de 10.

DESPUES DE ESTAS REGLAS Y CONSEJOS VAMOS A COMENTAR ASPECTOS A TENER EN CUENTA

Para empezar, lo que nunca tienes que hacer es utilizar contraseñas cortas que puedan obtenerse mediante ingeniería social, como el nombre de tu mascota, fechas importantes para ti o códigos postales. Tampoco hagas sustituciones clásicas como cambiar una e por un 3 o una o por un 0, ya que son trucos que los cibercriminales se conocen, y estate atento a las listas de las peores contraseñas para saber las que NUNCA tienes que utilizar.
No te centres en criterios y fórmulas predefinidas. Esto quiere decir que te olvides de que en una contraseña tienes que tener determinados caracteres alfanuméricos, que uno de ellos tiene que ser en mayúscula y que otro sea un símbolo. Todas estas fórmulas clásicas las saben también los cibercriminales, por lo que es una de las cosas que intentarán probar a la hora de adivinar la que tienes.

DESPUES DE ESTAS REGLAS Y CONSEJOS VAMOS A COMENTAR ASPECTOS A TENER EN CUENTA

También es importante que utilices contraseñas fáciles de recordar pero difíciles de adivinar. Un medio muy eficaz es el de utilizar combinaciones de varias palabras, que aunque aparentemente no tengan relación lógica entre ellas tú puedas relacionar para recordar.

Se ha comprobado que esta técnica es más efectiva que la de simplemente combinar mayúsculas, minúsculas, números y caracteres especiales en una contraseña corta. Estas no sólo son fórmulas predefinidas de esas que ya hemos recomendado no utilizar, sino que acaban siendo tan intrincadas que a veces acaban siendo tan difíciles de recordar que pierden todo el sentido.

Lamentablemente, hoy en día de poco sirve haber tomado las molestias oportunas para crear una buena contraseña si luego no las gestionamos correctamente, lo que a medio y largo plazo puede llevar a minimizar su eficacia. Por eso, ahora te dejamos una serie de pasos que es importante dar tras crear la contraseña para mantener tus cuentas seguras.

Una de las recomendaciones principales es no reutilizar las contraseñas en más de una web. Intenta tener una contraseña diferente en cada web, para que si alguien consigue descifrar una de tus contraseñas o la obtiene gracias a una filtración no pueda utilizarla para acceder a tus cuentas en más de una web o servicio online.

Programa universitario 50 plus José Saramago

DESPUES DE ESTAS REGLAS Y CONSEJOS VAMOS A COMENTAR ASPECTOS A TENER EN CUENTA

Intenta no compartir tus contraseñas con nadie más, ya que al hacerlo aumentas considerablemente las posibilidades de que caigan en malas manos. Esto puede ser porque la propia persona con la que las compartas las utilice para acceder a tus cuentas, pero también porque no sepa mantenerlas guardadas de forma segura y un tercero acabe conociéndolas.

Es importante cambiar tus contraseñas cada cierto tiempo. Proteger tus contraseñas no siempre depende de ti al 100%, ya que puede haber filtraciones que las expongan online. Por eso es importante ir cambiando tus contraseñas para que en el caso de que estas acaben filtrándose evites que alguien pueda utilizarlas.

En este sentido, también es recomendable mirar periódicamente páginas como Have I been pwned. Se trata de una veterana web que recopila todas las filtraciones de contraseñas. En ella, sólo escribes tu correo electrónico y la web te dice si se ha filtrado alguna contraseña en servicios en los que lo has utilizado. De esta manera, si ves que ha habido una filtración puedes prevenir y empezar a cambiar contraseñas.

Y ya que hablamos de correos, también es recomendable utilizar varias cuentas de correo para registrarte en las diferentes webs. Los correos se utilizan como identificadores, y si utilizas varios minimizarás el impacto que podría tener el que alguien acceda a uno de ellos. Por ejemplo, puedes tener un correo para servicios de uso personal, otro para los relacionados con el trabajo, e incluso un tercero para aplicaciones menos importantes.

DESPUES DE ESTAS REGLAS Y CONSEJOS VAMOS A COMENTAR ASPECTOS A TENER EN CUENTA

Utiliza siempre que puedas el doble factor de autenticación. Se trata de la verificación en dos pasos, una opción de seguridad que ofrece la mayoría de grandes servicios como WhatsApp, y que hace que para terminar de identificarte en un servicio necesites un segundo paso después de introducir la contraseña.
El segundo paso que se requiere depende del servicio. Algunos te envían un código por SMS que tienes que introducir después de la contraseña, aunque no es el método más seguro, mientras que otros te piden crear un pin o interactuar con la misma aplicación utilizando otro dispositivo como el móvil. Aunque suene molesto, es importante activarlo si de verdad no quieres que entren en tu cuenta.
Y por último, ante cualquier duda utiliza aplicaciones de terceros para gestionar tus contraseñas. Es posible que tras haber leído todos estos consejos te dé un poco de pereza hacerlos todos, algo que puede poner en peligro tu seguridad online. Es ahí donde entran en juego los gestores de contraseñas para hacer todo esto por ti.

Estos gestores de contraseñas se encargarán de crear por si mismos contraseñas robustas para los servicios online en los que estás registrado, e incluso las van cambiando periódicamente. Al utilizarlo pasarás de tener que recordar varias contraseñas a una única contraseña maestra. Eso sí, también es importante ir cambiando periódicamente las contraseñas de estos gestores y aplicar en ellos todos nuestros consejos, ya que de ellos depende la seguridad del resto de tus cuentas.

Programa universitario 50 plus José Saramago

DETALLE 6.0
EL MODO AVION

Se puso en marcha en 2013 para permitir que los aparatos electrónicos no fuesen apagados durante todas las fases del vuelo. De esta manera, los usuarios pueden ir trabajando, por ejemplo, con documentos mientras realizan ese viaje de negocios, escuchar música o leer.

Y es que esta opción corta las conexiones inalámbricas del terminal. (Todas las señales que realiza el móvil a través de las ondas son canceladas). Es decir, un «móvil» se queda sin datos y línea cuando activa este modo, pero sí podemos realizar otras acciones.

Recordar que la función mas normal del móvil es el uso de datos, solo cuando se encuentra muy cerca de un emisor de Wifi, y tiene autorización (la clave del wifi) se conecta por wifi.

En estos momentos la Autoridad Europea de Seguridad Aérea (EASA) permite y se trata solo de un primer paso de usar con todos las funciones de los móviles y permite la generalización del uso de estos dispositivos durante en el vuelo ya que el siguiente reto es habilitar la conexión a internet dentro del avión mediante un sistema de telefonía móvil o wifi especifico.

En modo avión desactivado hace que, el aparato deja de transmitir señales (las señales son las ondas que emite) que puedan interferir con los sistemas del avión. Incluso activar el wifi, pero, te quedas sin la señal (onda), así que de poco te servirá.

SILENCIAR EL TELEFONO

Silenciar el teléfono es la posibilidad que los sonidos que emiten los teléfonos no solo los distintos tonos de llamadas, de notificaciones y otros puedan ser percibidos por nosotros. Lo que en realidad hacemos es enmudecer cualquier sonido que emite el teléfono.

Esta situación es administrada por nosotros dentro de Ajustes, también podemos acceder a través de la tecla que tenemos en la parte del costado del teléfono donde se puede variar el volumen de los sonidos del teléfono, habitualmente aparecen una campana y una luna que nos permite sin llegar a los ajustes, colocar si pulsamos la campana en modo de silencio, y si pulsamos la luna activar el no molesten.

Estas son opciones donde se interrumpe los sonidos que se emiten a través del altavoz del móvil. El modo de no molestar (DND) es una de las mejores características de Android

Dentro de las posibilidades de ajustes de sonido, que tenemos según los modelos de teléfonos, está la opción de vibración, que nos permite conocer que tenemos alguna llamada, sin ningún ruido (sonido) que perturbe a los que nos rodean.

Si usamos la aplicación de ajustes (la rueda dentada), tendremos que buscar el punto que marca como “SONIDO Y VIBRACION”, dentro del cual tenemos otras opciones referentes al sonido de multimedia (música principalmente), El tono de llamada (según el modelo podemos indicar la melodía con la cual queremos recibir una llamada) de igual forma el sonido de la alarma como despertador.

Programa universitario 50 plus José Saramago

SILENCIAR EL TELEFONO

Dentro de este apartado podemos programar la activación o el tiempo de duración de silenciar el teléfono, y apartados como “NO MOLESTAR”, “NOTIFICACION DE LLAMADAS”, “VIBRAR EN LAS LLAMADAS”, “VIBRAR EN MODO DE SILENCIO” y otros ajustes adicionales, así como los efectos sobre el sonido.

Los consumos de la batería en modo de silencio son menores, aunque su apreciación es difícil de evaluar.

Programa universitario 50 plus José Saramago

DETALLE 7.0
QUE ES UNA CUENTA DE CORREO ELECTRÓNICO Y COMO OPERA

Una cuenta de correo electrónico es un servicio en línea que proporciona un espacio para recibir, enviar y almacenar mensajes de correo electrónico en Internet. Cada cuenta de correo electrónico se asocia a un único usuario, que puede acceder a su cuenta a través de un nombre de usuario y contraseña. La cuenta de correo electrónico es como una dirección de correo en Internet Para enviar o recibir mensajes de correo electrónico, es necesario tener una cuenta de correo electrónico, que es un buzón virtual identificado por una dirección de correo electrónico. La dirección de correo electrónico tiene un formato de tres partes distintas: una parte local, un símbolo "@" y un dominio. Las empresas, administraciones, centros educativos y proveedores de servicios de Internet suelen proporcionar cuentas de correo electrónico. El correo electrónico es el método más estandarizado para enviar y recibir mensajes.

Tipos de cuentas de correo

Empezaremos por lo más básico. Generalizando, las cuentas de correo electrónico pueden ser personales o corporativas. Te mostraré un poquito sobre la importancia de tener las dos.

Email corporativo

Ya sea que tengas un negocio propio, trabajes para una empresa o seas freelancer, nunca debes mezclar lo personal con lo profesional. Ya debes haber escuchado esto muchas veces. Pues debo decirte que con el email funciona de la misma forma.

Una cuenta de correo electrónico es un servicio en línea que proporciona un espacio para recibir, enviar y almacenar mensajes de correo electrónico en Internet. Cada cuenta de correo electrónico se asocia a un único usuario, que puede acceder a su cuenta a través de un nombre de usuario y contraseña. La cuenta de correo electrónico es como una dirección de correo en Internet Para enviar o recibir mensajes de correo electrónico, es necesario tener una cuenta de correo electrónico, que es un buzón virtual identificado por una dirección de correo electrónico. La dirección de correo electrónico tiene un formato de tres partes distintas: una parte local, un símbolo "@" y un dominio. Las empresas, administraciones, centros educativos y proveedores de servicios de Internet suelen proporcionar cuentas de correo electrónico. El correo electrónico es el método más estandarizado para enviar y recibir mensajes.

Tipos de cuentas de correo

Empezaremos por lo más básico. Generalizando, las cuentas de correo electrónico pueden ser personales o corporativas. Te mostraré un poquito sobre la importancia de tener las dos.

Email corporativo

Ya sea que tengas un negocio propio, trabajes para una empresa o seas freelancer, nunca debes mezclar lo personal con lo profesional. Ya debes haber escuchado esto muchas veces. Pues debo decirte que con el email funciona de la misma forma.

Un email corporativo, además de ayudarte en la organización, te sirve para darle un aspecto más profesional a tu negocio, independientemente de cuál sea. De esta forma, también evitas la distracción que te puede traer el recibir emails personales mientras estás trabajando.

Email personal

Este email puedes utilizarlo para todo lo que quieras. Participar de las redes sociales, registrarte en diferentes sitios webs, suscribirte a todas las newsletters que te interesen, comunicarte con tus amigos y familia, etc.

Al tener una cuenta de email personal, no corres el riesgo de que emails profesionales se pierdan entre una gran cantidad de emails personales.

Programa universitario 50 plus José Saramago

Tipos de proveedores de email

Es importante conocer los principales proveedores de email ya que cada uno tiene algunas funcionalidades que para ti pueden ser más útiles que otros. Veamos los 3 principales.

Gmail

El servicio de correo electrónico de Google actualmente es uno de los más populares en todo el mundo. Tiene muy buenos recursos de organización y elimina los correos no deseados con facilidad.

Debido a su éxito, la desventaja es que difícilmente puedes encontrar nombres disponibles. Si quieres crear un email con tu nombre, debes agregarle números o símbolos.

Outlook

Si naciste antes del 2000, lo más probable es que en algún momento de tu vida hayas tenido una cuenta de Outlook. ¿No lo crees? ¿Nunca has tenido una cuenta de Hotmail?

Actualmente no es tan utilizada, pero hubo una época en que era muy popular. Bueno, desde el 2012 Hotmail pertenece a Outlook.

Outlook es uno de los proveedores de email más populares. Es el servicio de correo electrónico gratuito de Microsoft. Su gran ventaja es que se integra fácilmente con las aplicaciones de Microsoft.

Yahoo! Mail

Ya fue mucho más popular que ahora, pero a pesar de eso continúa siendo muy utilizado.

Uno de los factores es su fácil integración con Facebook y la posibilidad de crear emails desechables que permiten una mayor privacidad.

Sin embargo, algo con lo que hay que tener cuidado es que, si no utilizas tu cuenta por más de 4 meses seguidos, está será desactivada automáticamente.

DETALLE 8.0
POSIBLES ESTAFAS Y TELEFONOS DE AYUDA

Estos son algunos de los posibles casos, para robarnos datos personales, haciéndose pasar por entidades o empresas legales.

POSIBLES CASOS

1.Emails o SMS que se hacen pasar por Correos (y otras empresas de mensajería)
2. Falsos emails de la Agencia Tributaria (y otros organismos oficiales)
3. Falsos códigos de verificación de WhatsApp
4. Falsos comunicados sobre el covid
5. Confirmaciones de pedido de Amazon
6. Phishing de bancos y servicios de pago
7. Robo de cuentas en Instagram
8. Phishing de servicios de videoconferencia o clases online
9. Estafas con criptomonedas
10. Phishing de plataformas de streaming (Netflix, Amazon Prime, HBO o Disney Plus)
11. No te acuerdas de mi...?

Programa universitario 50 plus José Saramago

RECORDAR

- Ante cualquier duda, borrar mensajes sin abrirlos.
- Si se trata de empresas, procurar visitar a la empresa en los locales que tiene habilitados para atención directa, no hay prisa y podemos hacerlo, si tenemos impedimento físico enviar a alguien de nuestra confianza.
- Las criptomonedas no son para nosotros si necesitamos alguna actividad económica directamente con las entidades financieras donde tengamos nuestros depósitos.
- Los falsos comunicados sobre covid, guerras, ayudas a las ong´s, y otros organismos, dejemos pasar todos esos comunicados y si queremos ayudar a los demás empecemos por nosotros mismos, y luego vayamos a los sitios donde están representados los organismos y preguntemos.
- Los pedidos a empresas, si se han realizado los pedidos, ya saben cómo tienen que entregar los pedidos, y si no ya insistirán, dejémosle que tengan interés. Pero si no hay pedidos ni caso.
- Los códigos de verificación o doble verificación se realizan al instante y en el origen te explican cómo se realizan, por lo tanto, si no se está haciendo ninguna operación en donde se necesite esa doble verificación es que algo no va bien. No dar ningún dato personal.

Programa universitario 50 plus José Saramago

RECORDAR

- Recordar que las páginas web que tiene seguridad empiezan por https eso nos da una pista, pero verificar si nos llevan a otra página viendo el enlace.
- No te acuerdes de nadie que lleves tiempo sin tener noticias y menos le dices algo al respecto.
- Las llamadas telefónicas de empresas de teléfono, luz, entidades bancarias, ya conocen nuestros datos, por lo tanto, cuando empiecen a preguntar nuestro domicilio y algún dato más, sospechar de esa llamada.
- Llevar tarjeta de pago bancario con límite de pago, o bien tarjetas virtuales, las claves nunca al alcance de nadie, en nuestra caja fuerte rápida “la cabeza”.
- Al sacar dinero de cajeros, comprobar con una mirada lo que tenemos alrededor, llevar la tarjeta previamente sacada de la cartera o bolso, y nunca desentender lo que estamos haciendo porque alguien nos indique o pregunte algo, primero nuestras cosas y luego la de los demás.
- Los bolsos en bandolera y en la parte delantera de nuestro cuerpo.

NUNCA DAR INFORMACION PERSONAL POR TELEFONO, NI POR NINGUN MEDIO, SIN SER CONTRASTADO

Programa universitario 50 plus José Saramago

DETALLE 9.0
BIZUM

Bizum es uno de los servicios de pago instantáneo más conocidos del sector de la banca online. Su inmediatez, gratuidad y facilidad de uso ha convencido a más de 15 millones de usuarios.

Creado en 2016, Bizum es propiedad de la empresa Sociedad de Procedimientos de Pago SL.

Bizum es un servicio de pago instantáneo que avala el propio Banco Central Europeo (BCE). Se asemeja a una trasferencia instantánea, sin comisiones.

"Si llevas un móvil, llevas dinero encima", este es el lema de Bizum,

Bizum funciona de manera muy sencilla y opera de forma gratuita.

Por ejemplo, un usuario entra en su banca online, selecciona la pestaña de la plataforma, escribe el importe, el número de teléfono (OJO con los números de teléfono que tiene números delante con el código de país, sobre todo en nuestra lista de contactos) y hace clic en enviar.

La única condición que tenemos en Bizum es que debemos poseer de una cuenta bancaria activa en el banco donde queremos utilizar este servicio y tener asociado nuestro número de teléfono móvil a dicha cuenta.

Programa universitario 50 plus José Saramago

Hay que saber que hay límites a las cantidades que se encuentren entre 0.50 a 1.000 €, para poder realizar un Bizum, al igual que el número de veces. Todo depende del banco (plataforma) y sus condiciones.

Hacer un Bizum es muy sencillo, aunque el proceso depende de cuál del banco en el que se tenga la cuenta corriente. En la actualidad, más de 30 entidades (plataformas) están adheridas a esta plataforma con la diferencia de que algunas optan por integrarla dentro de banca online y otros por crear una app (Aplicación) específica para la suya.

Los Bizum que se envían a otro usuario por error no se pueden anular.

Si se puede negar la petición de dinero que te solicitan, sin ningún problema.

El tiempo que tarda en llegar un bizum es de aproximadamente 5 segundos. SI alguien te hace una petición, tienes un plazo de hasta 7 días para aceptarlo o, en su defecto, para rechazarlo.

Tanto si recibes un ingreso o una solicitud de un número desconocido, lo primero que tienes que hacer es desconfiar y luego ¡llamar a tu banco! Así podrás descubrir la identidad del usuario o detectar si se trata de una posible estafa online.

Hoy en día, las estafas online (smishing, vishing y phishing) tienen en vilo a la seguridad de todo el país.

Conclusión a tener en cuenta:

-En nuestros contactos tener el número de teléfono bien definido, incluido el apartado de país. (+ 34 es España)

-Denegar si procede la petición de dinero cuando se solicita, si no conocemos el origen o procedencia.

-Nunca permitas transacciones sino son conocidas, ponte en contacto con tu banco.

-Los Bizum no se pueden anular.

Programa universitario 50 plus José Saramago

DETALLE 10.0
CUIDADO SI PAGAS CON EL MÓVIL

TE PUEDEN ROBAR TODO EL DINERO DE TU CUENTA

Ten cuidado al pagar con el móvil si no quieres que te roben tu dinero.

La tecnología NFC (Near Field Communication) (Comunicación con el campo más cercano) se ha convertido en un compañero cotidiano para muchos usuarios de teléfonos móviles en los últimos años. Este avance tecnológico ha transformado la forma en que realizamos pagos, simplificando nuestras transacciones diarias y eliminando la necesidad de llevar consigo una cartera llena de tarjetas de crédito o débito. Sin embargo, con la conveniencia que ofrece, también emergen riesgos asociados con la seguridad financiera personal.

Aviso si pagas con el móvil

El Banco de España, consciente de esta evolución en los hábitos de pago, ha lanzado una serie de recomendaciones dirigidas a los consumidores para salvaguardar la seguridad al utilizar esta tecnología. La intención es brindar directrices claras y prácticas que permitan aprovechar los beneficios de la tecnología NFC sin exponerse a posibles riesgos financieros.

Programa universitario 50 plus José Saramago

Ten cuidado al pagar con el móvil si no quieres que te roben tu dinero.

Una de las principales sugerencias del Banco de España es configurar medidas de seguridad en el dispositivo móvil. Establecer un sistema de bloqueo mediante un código, patrón o huella dactilar es esencial para evitar accesos no autorizados. Además, se recomienda implementar un doble factor de autenticación para acceder a la cartera digital, añadiendo una capa extra de protección. KO del jueves, 4 de enero de 2023.

Otra sugerencia clave es fijar un límite mínimo para que sea necesario introducir el PIN de la tarjeta al realizar pagos. Esta medida de seguridad adicional garantiza que, aunque alguien tenga acceso físico al móvil, no pueda realizar transacciones de alto valor sin la debida autorización.

Además, el Banco de España aconseja desactivar la función NFC del móvil cuando no se esté utilizando para realizar pagos. Esta precaución extra puede evitar posibles intentos de acceso no autorizado a través de esta tecnología de comunicación cercana.

Programa universitario 50 plus José Saramago

Estafas que te dejarán sin dinero

Pero por desgracia, la ciberdelincuencia sigue evolucionando y cada vez existen más formas de que puedan robarte tu dinero. Las tácticas más comúnmente empleadas por los delincuentes cibernéticos son las siguiente:

- Fraude mediante técnicas como el phishing (Suplantacion de Identidad), smishing (Sonriendo), vishing (Vistiendo) o el shoulder surfing (hombro de surf). Estos métodos implican engaños para obtener información confidencial, ya sea a través de mensajes electrónicos, llamadas telefónicas, o la observación directa de información sensible.
- Distribución de malware diseñado para capturar las pulsaciones del teclado. Estos programas maliciosos son capaces de registrar y transmitir la información introducida por el usuario, comprometiendo así la seguridad de contraseñas y datos personales.
- Explotación de bases de datos de clientes que han sufrido brechas de seguridad y se encuentran publicadas en la deep (profundo) web. Estas bases de datos contienen información personal valiosa que puede ser utilizada para cometer fraudes.

Programa universitario 50 plus José Saramago

Estafas que te dejarán sin dinero

- Suplantación de sitios web legítimos a través de webs fraudulentas para obtener datos personales. Los ciberdelincuentes crean réplicas engañosas de sitios web auténticos para engañar a las personas y obtener su información confidencial.
- Uso de dispositivos de lectura con tecnologías inalámbricas como RFID o NFC para obtener datos de tarjetas. Estos dispositivos son capaces de leer información de tarjetas de crédito o débito sin necesidad de contacto físico, comprometiendo la seguridad de la información financiera.
- Skimming, (Hojeando) que implica el robo de datos de tarjetas bancarias mediante la manipulación de cajeros automáticos. Los delincuentes instalan dispositivos ilegales en los cajeros automáticos para copiar la información de las tarjetas utilizadas, permitiéndoles realizar transacciones fraudulentas.

Programa universitario 50 plus José Saramago

Fuentes consultadas:

http://www.ietf.org/proceedings
http://vig.pearsoned.com
http://www.webopedia.com
http://www.csr.com
http://www.howstuffworks.com
Wikipedia
https://www.xataka.com
https://areatecnologia.com
https://es.scribd.com
https://areatecnologia.blogspot.com