Cofinanciado por el programa Erasmus+ de la Unión Europea

ERASMUS KA226
2020-1-ES01-KA226-SCH-096012
Título: We are ready for digital word
ERASMUS KA122
2021-1-ES01-KA122-SCH-000012981
Título: ICT (tecnología de la información y las comunicaciones)

TALLER DE CIBERSEGURIDAD

IES SAN SEBASTIÁN (HUELVA)

Fecha: 21/03/22
Lugar: Aula 21
Dirigido a profesores del IES San Sebastián
Impartido: Olga López Fernández
Organiza: Programa Erasmus KA226 y KA122

Ante la delicada situación actual de incremento de los ciberataques y del cibercrimen, debemos entre TODOS fortalecer la ciberseguridad en todas las organizaciones públicas.

Para ello, te damos las siguientes RECOMENDACIONES:

- **Cambiar las contraseñas** de las cuentas de usuario, usando nuevas contraseñas con mayor complejidad, si cabe.
    - Longitud mínima de 8 caracteres de las siguientes categorías:
        - Letras mayúsculas y minúsculas, con o sin acentos.
        - Números (del 0 al 9)
        - Caracteres especiales (~! @ # $% ^& * -+ = ' | \ \ (){}\ []:; "' <>,.? /)
    - La contraseña no debe contener partes del nombre y apellidos, ni del nombre de usuario
- Se puede **comprobar si que utilizas es segura:**

https://password.kaspersky.com/es/

- Se recomienda, como medida preventiva, **apagar el equipo informático al finalizar la jornada** si éste no va a ser utilizado.

Por otro lado, te pedimos que estés atento en tu día a día y sigas las siguientes PAUTAS:

- Prestar especial **atención a los mensajes sospechosos por cualquier vía** (correo, Whatsapp, SMS...)
    - de remitentes poco frecuentes o inesperados
    - requiriendo actuaciones urgentes
    - habitualmente con mala redacción.
    - Especial cuidado con los ficheros adjuntos: ficheros ejecutables, documentos con macros...
- **No pulsar en enlaces** que provengan **de fuentes poco fiables**.
    - Pasar el ratón sobre el enlace y confirmar si parece legítimo.
    - Consultar con el departamento de informática en caso de duda.
- **No instalar aplicaciones dudosas o no corporativas** en los equipos o en los móviles.
- **Estar atentos a las notificaciones y seguir las recomendaciones** que se remitan **desde la Unidad de seguridad TIC** o el departamento de informática de vuestro organismo.
- **Remitir correos sospechosos a AndalucíaCERT** a través de la dirección abuse@juntadeandalucia.es
- **Ante comportamientos claramente maliciosos** en el equipo (imposibilidad de acceder a ficheros, mensajes en pantalla...) es recomendable desconectarlo de la red y **avisar al departamento de informática y/o Unidad de seguridad TIC**.

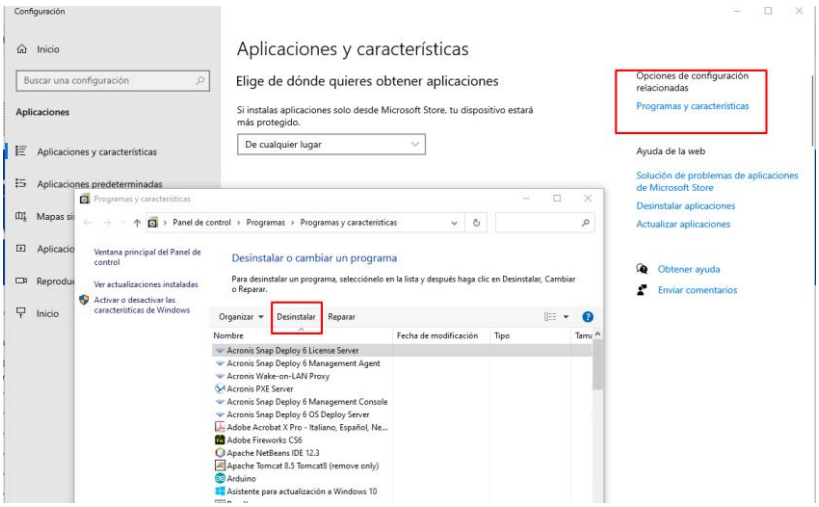
HAZ QUE TU ORDENADOR SEA MÁS SEGURO

https://www.redeszone.net/tutoriales/seguridad/consejos-hardening-ordenador-windows-10/

os vamos a realizar una serie de **recomendaciones básicas** que puedes hacer para que configures Windows con la mejor seguridad posible, todas estas sugerencias son muy fáciles de realizar y aptas para todos los usuarios.

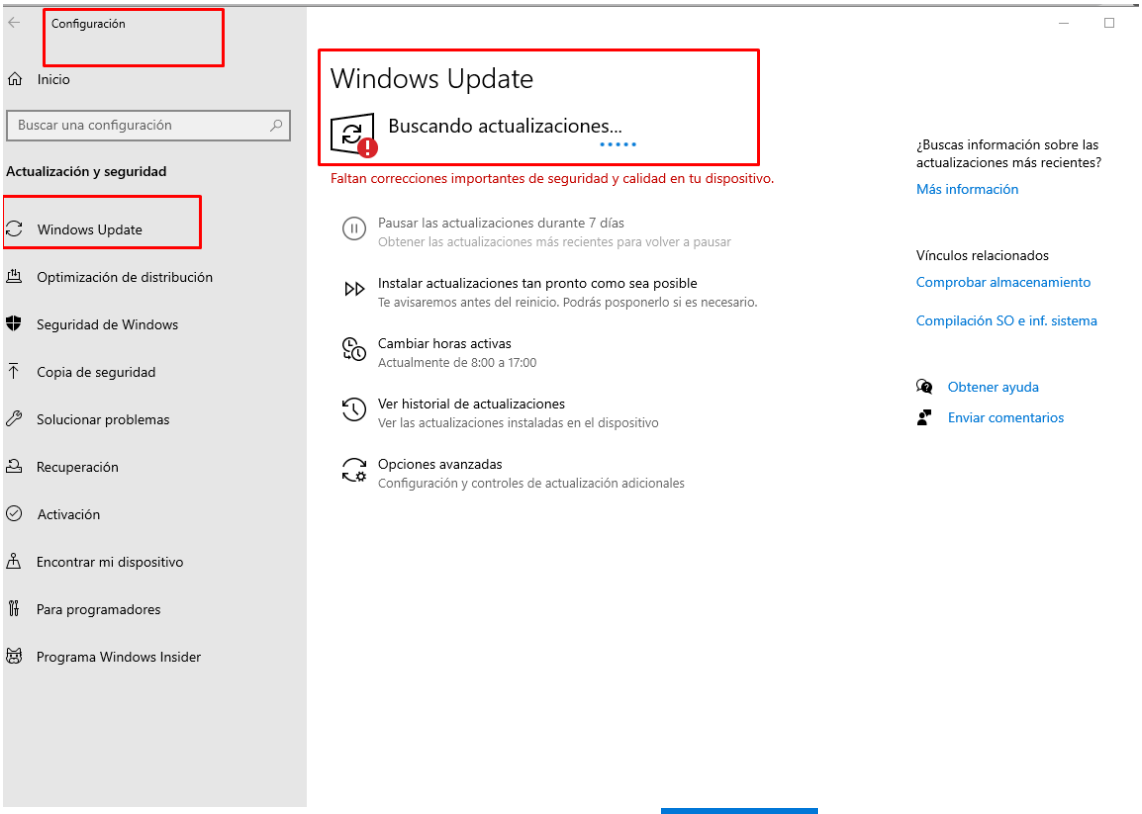
Desinstalar programas que no estemos usando

¿Cómo gestiono mis programas? Simplemente, dirígete al menú y busca la frase «agregar o quitar programas». Selecciona dicha opción y te dirigirá directamente al listado de programas instalados.



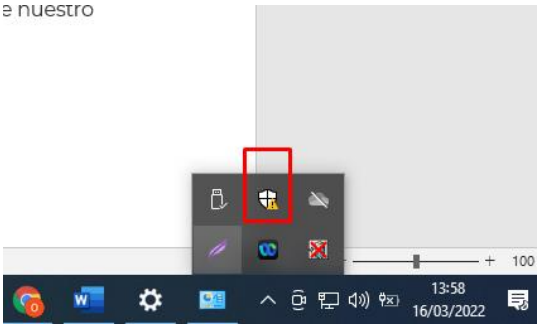
¡!IMPORTANTE!! Tener siempre el Windows actualizado

https://www.andaluciacompromisodigital.org/recurso/taller-online-consejos-para-mantener-windows-10-mas-seguro/



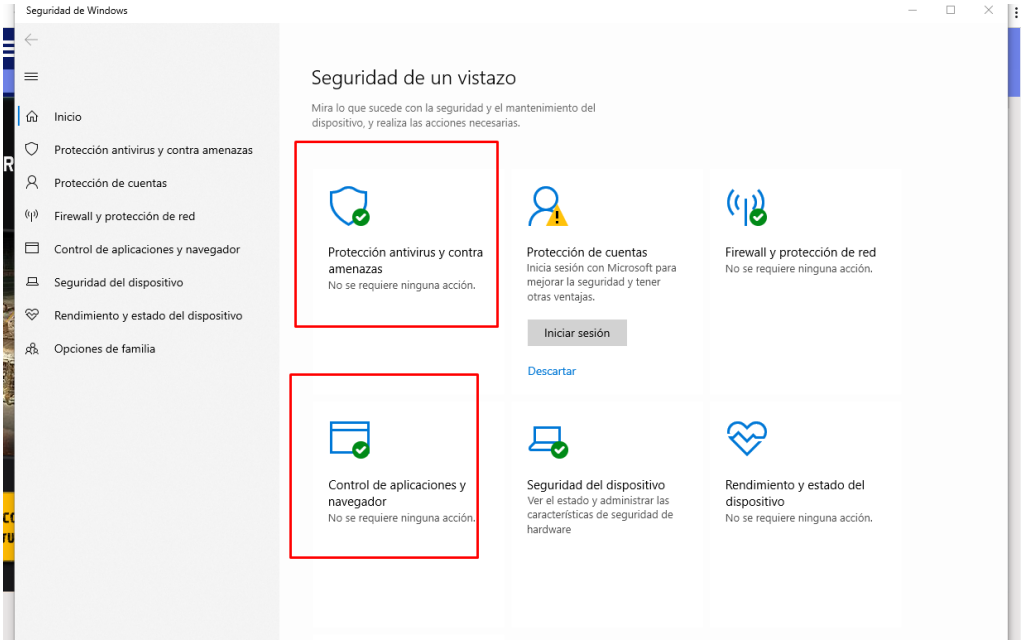
Utilizar Seguridad de Windows –Windows Defender

A esta herramienta se la conoce también como **Windows Defender**. Esta solución puede ser la gran desconocida, pero en los últimos tiempos ha mejorado muchísimo y es actualmente la solución antivirus/antimalware más recomendable de usar, además, es completamente gratis y viene incorporada en nuestro sistema operativo. A pesar de que ya cuenta con ciertas prestaciones activadas por defecto, se considera como buena práctica el poder personalizar los ajustes de los mismos de manera a proteger más eficazmente nuestro ordenador.

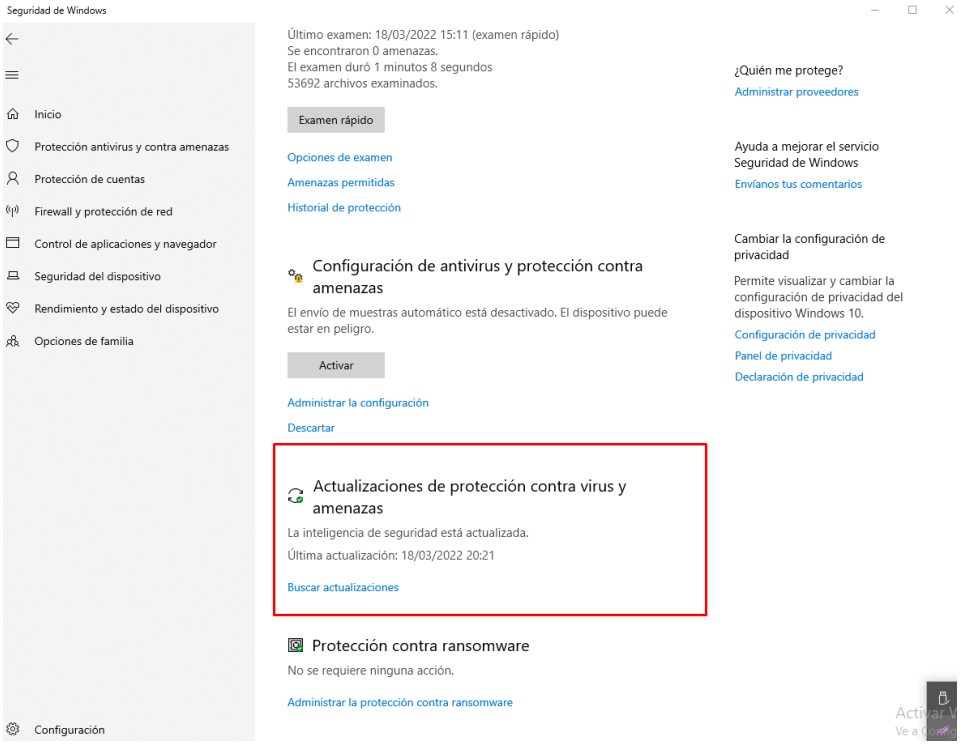


Existen opciones que merecen especial atención, una de ellas es la de **Protección contra virus y amenazas**. Al momento de ingresar, tendrás la posibilidad de realizar un examen rápido de los archivos contenidos en tu ordenador. Esto toma unos pocos minutos y te detalla el número de amenazas encontradas si las hubiere. Así también, es posible personalizar los exámenes con variantes como el **examen completo** o el **examen de Windows Defender sin conexión**.

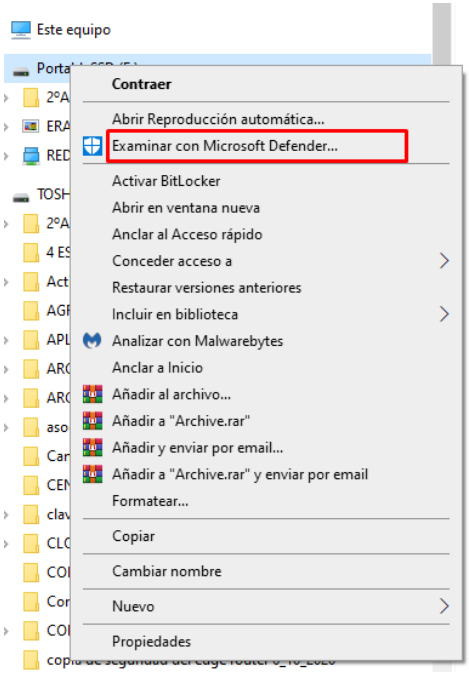
Por otro lado, es válido fijarse en la opción de **Rendimiento y estado del dispositivo**. En la misma podemos tener un vistazo sobre cómo se encuentra nuestro ordenador. Te dará información respecto al estado de la batería, capacidad de almacenamiento y otros aspectos más. Si tus necesidades no pasan de lo esencial, no necesitas descargar alguna solución de seguridad adicional.



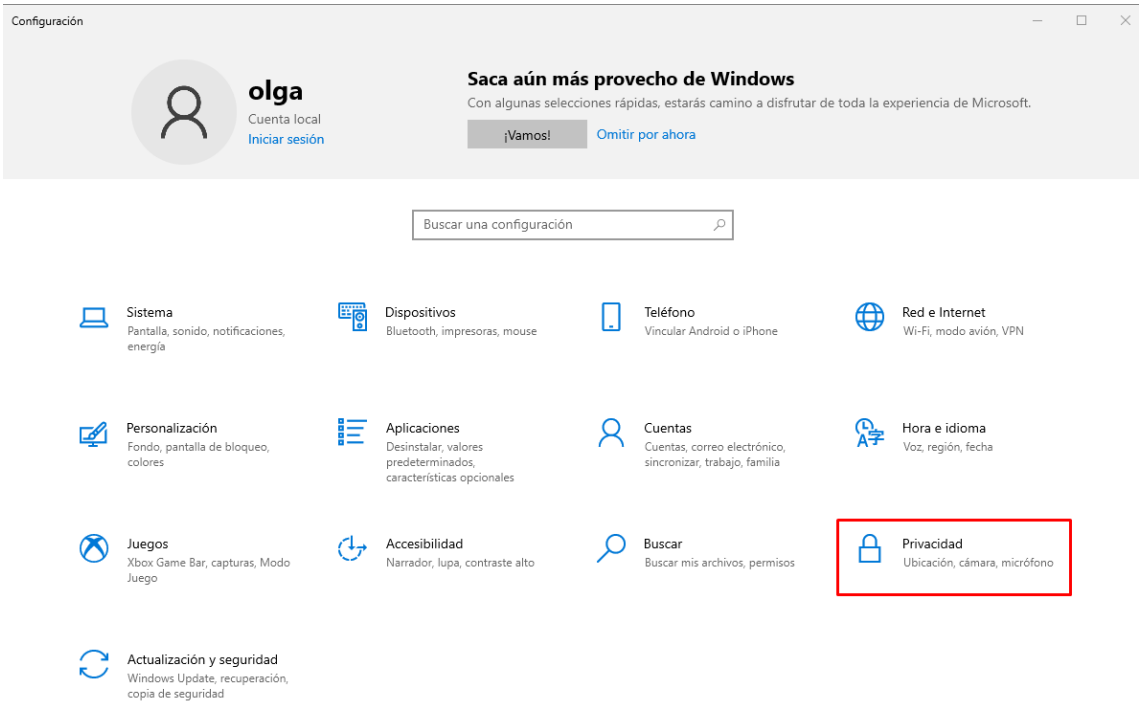
Tener siempre las actualizaciones al día

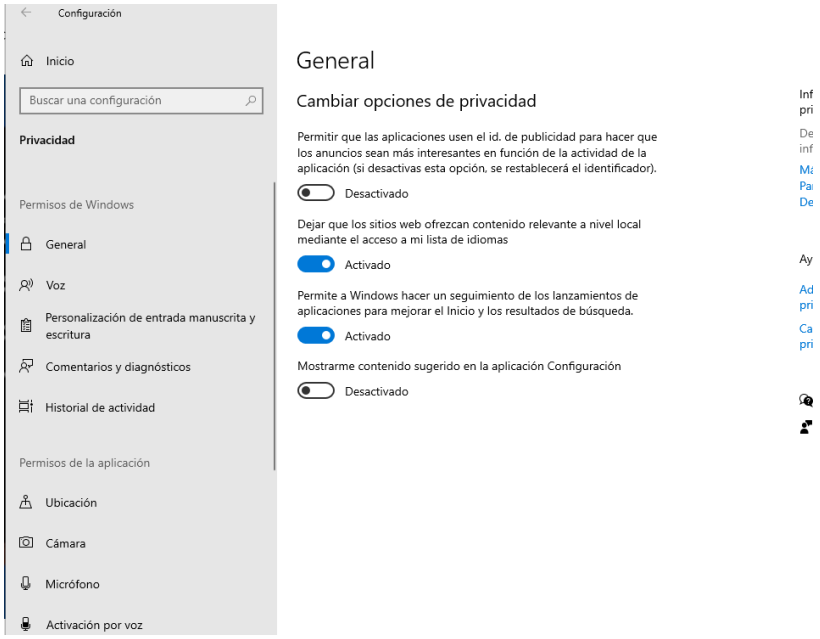


Cómo examinar nuestro USB con Windows defender

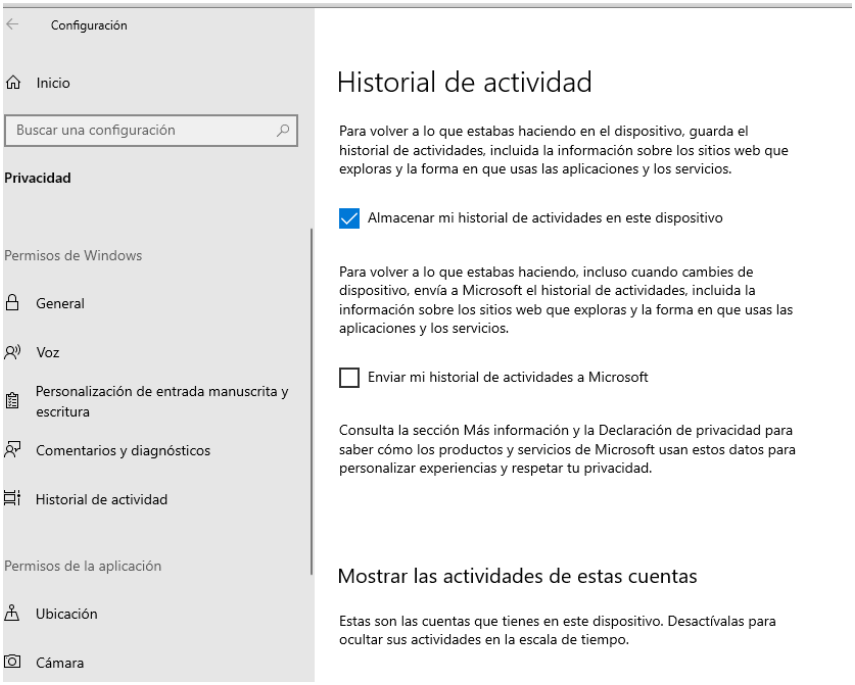


PRIVACIDAD de nuestro equipo

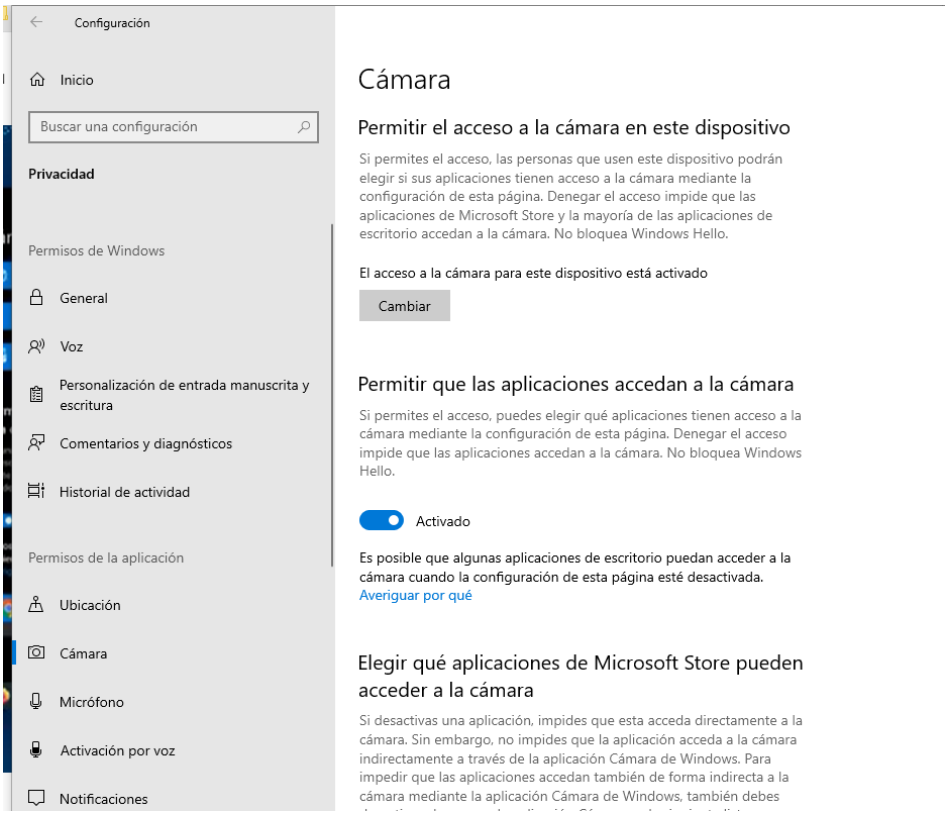

Configuración
olga
Cuenta local
Iniciar sesión
Saca aún más provecho de Windows
Con algunas selecciones rápidas, estarás camino a disfrutar de toda la experiencia de Microsoft.
¡Vamos!
Omitir por ahora
Buscar una configuración
Sistema
Pantalla, sonido, notificaciones, energía
Dispositivos
Bluetooth, impresoras, mouse
Teléfono
Vincular Android o iPhone
Red e Internet
Wi-Fi, modo avión, VPN
Personalización
Fondo, pantalla de bloqueo, colores
Aplicaciones
Desinstalar, valores predeterminados, características opcionales
Cuentas
Cuentas, correo electrónico, sincronizar, trabajo, familia
Hora e idioma
Voz, región, fecha
Juegos
Xbox Game Bar, capturas, Modo Juego
Accesibilidad
Narrador, lupa, contraste alto
Buscar
Buscar mis archivos, permisos
Privacidad
Ubicación, cámara, micrófono
Actualización y seguridad
Windows Update, recuperación, copia de seguridad


Configuración
Inicio
Buscar una configuración
Privacidad
Permisos de Windows
General
Voz
Personalización de entrada manuscrita y escritura
Comentarios y diagnósticos
Historial de actividad
Permisos de la aplicación
Ubicación
Cámara
Micrófono
Activación por voz
General
Cambiar opciones de privacidad
Permitir que las aplicaciones usen el id. de publicidad para hacer que los anuncios sean más interesantes en función de la actividad de la aplicación (si desactivas esta opción, se restablecerá el identificador).
Desactivado
Dejar que los sitios web ofrezcan contenido relevante a nivel local mediante el acceso a mi lista de idiomas
Activado
Permite a Windows hacer un seguimiento de los lanzamientos de aplicaciones para mejorar el Inicio y los resultados de búsqueda.
Activado
Mostrarme contenido sugerido en la aplicación Configuración
Desactivado

HISTORIAL de actividad



CÁMARA



SERVICIO ANTIBOTNET

Una botnet o red zombi es un conjunto de dispositivos controlados remotamente por un ciberdelincuente. Los dispositivos infectados por la botnet pertenecientes a la empresa pasarán a ser controlados por los ciberdelincuentes, poniendo en riesgo la privacidad y seguridad de tu empresa.

https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet

MALWAREBYTES

Malwarebytes

RECOMENDACIONES

- Recomendaciones a tener en cuenta en relación a las soluciones anti-malware:
- Mantener los sistemas actualizados y libres de virus y vulnerabilidades. de este modo estaremos protegidos frente ataques, malware, etc;
- Concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen software sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa;
- Mantener actualizado los sistemas operativos y aplicaciones;
- Evitar la descarga e instalación de programas desde sitios web que no ofrezcan garantías; utilizar redes seguras para todas las comunicaciones con nuestros clientes. y emplear cifrado cuando la información intercambiada sea especialmente sensible;
- Realizar copias periódicas de seguridad que incluyan los datos del cliente que debamos proteger. también debemos tener procedimientos de restauración de dichas copias.

Malwarebytes

Descarga de

Google Drive

GOOGLE DRIVE EN PC

Para sincronizar con Google Drive, o crea una copia de seguridad en Google Fotos y accede a todo el contenido directamente desde una PC o una Mac

Imagen de nuestro equipo

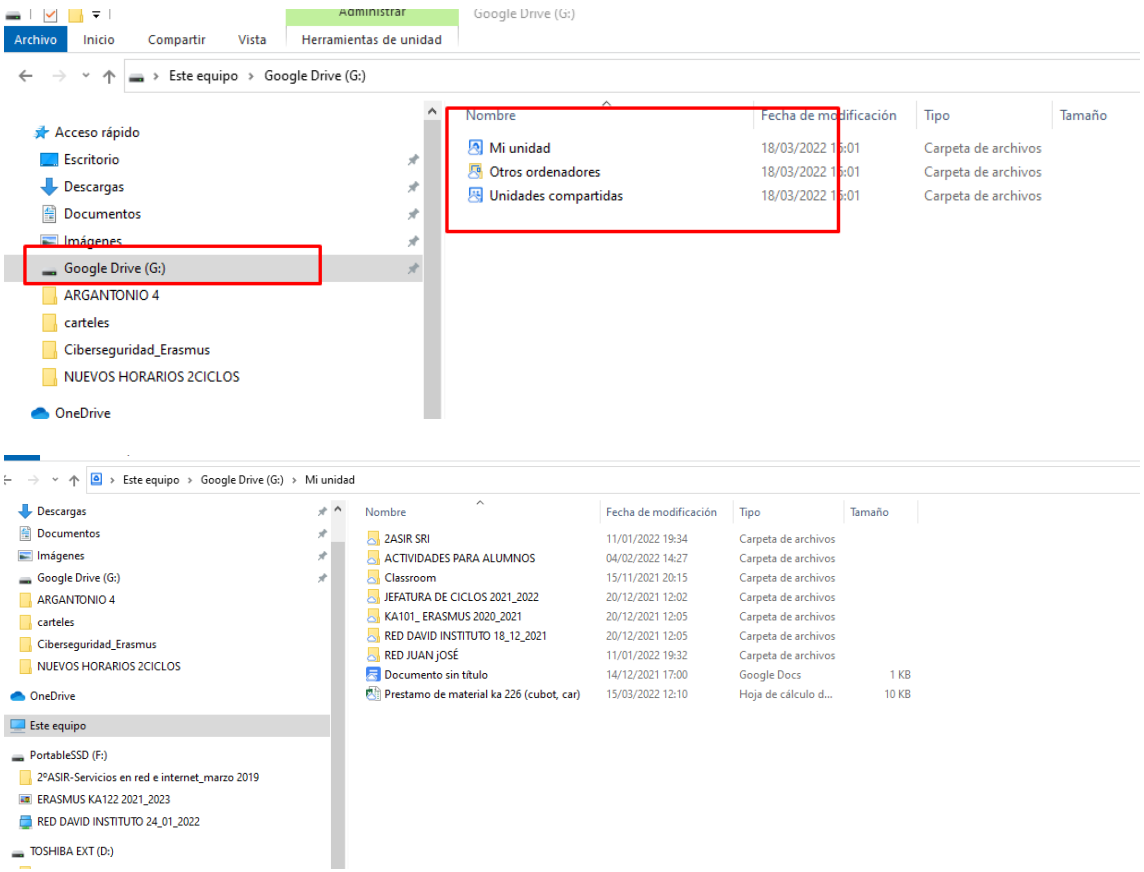
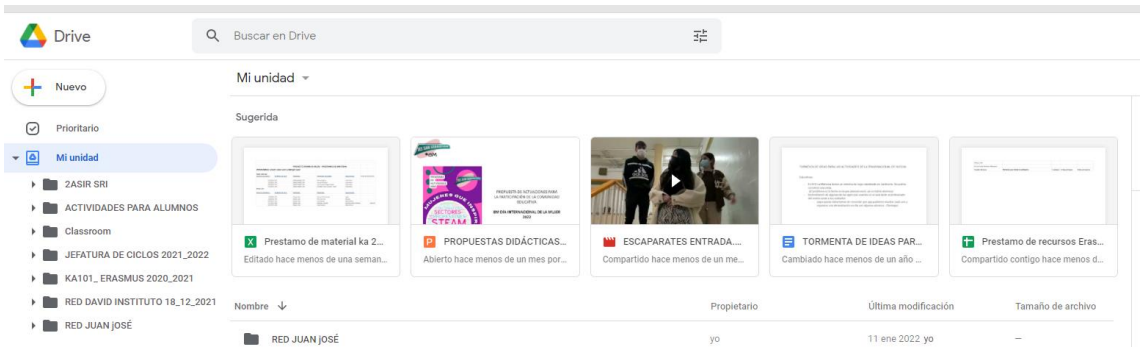
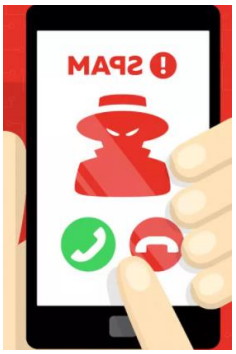


Imagen de la Web



SEGURIDAD EN NUESTRO MÓVIL

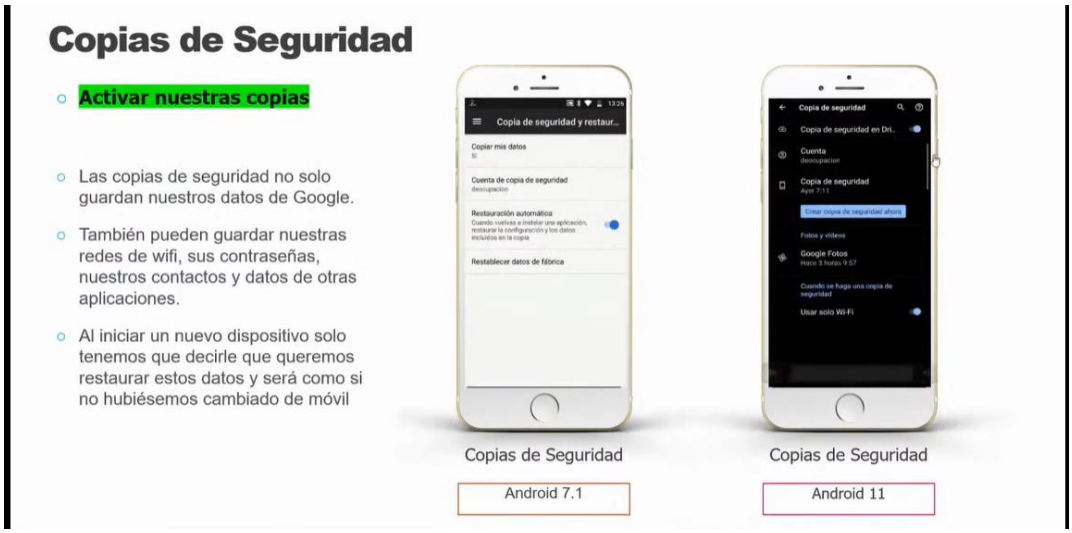


https://www.andaluciacompromisodigital.org/recurso/taller-seguridad-dispositivo-movil/

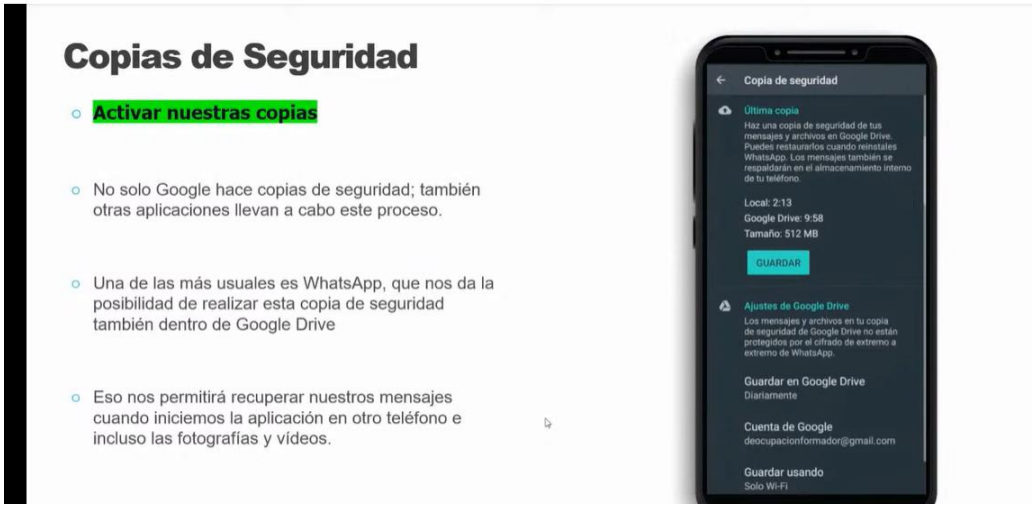
- Controlar tu acceso a tu tarjeta SIM
- No desactivar la opción PIN de la tarjeta
- Controlar tu acceso a tu móvil
- Descargar aplicaciones oficiales (investigar antes sobre esa aplicación)
- No conectarte a wifi desconocidas
- Desactivar el NFC, bluetooth, GPS, zona wifi, wifi

Trampa wifi

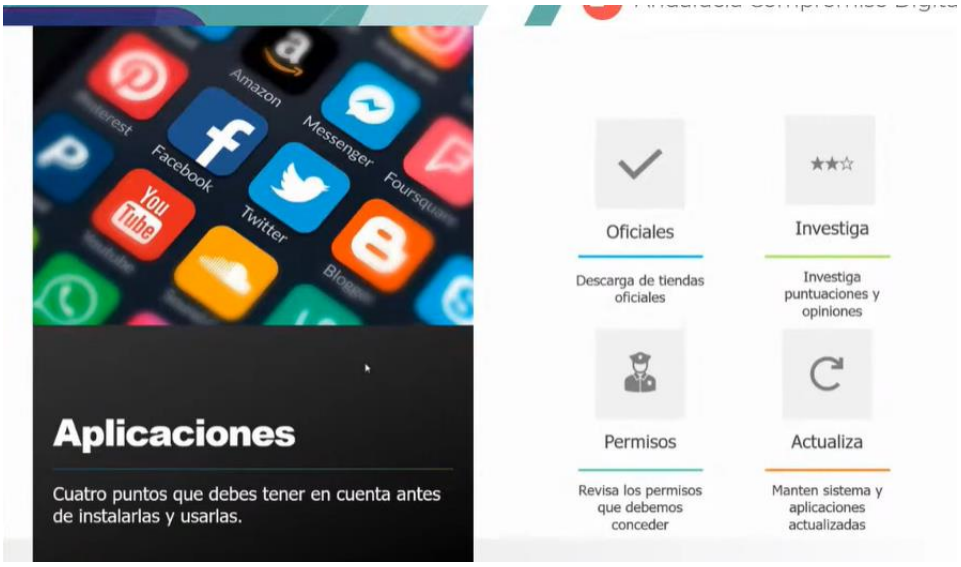
Copias de seguridad

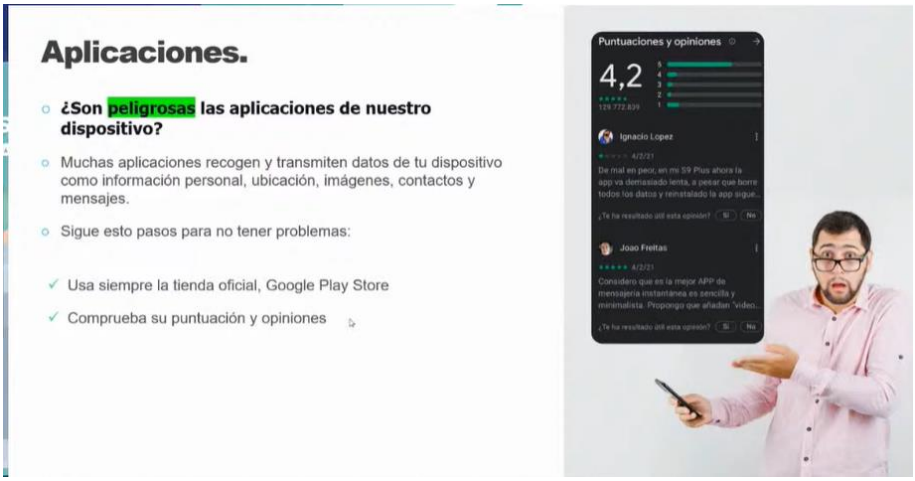


Copia de seguridad en Whatsapp

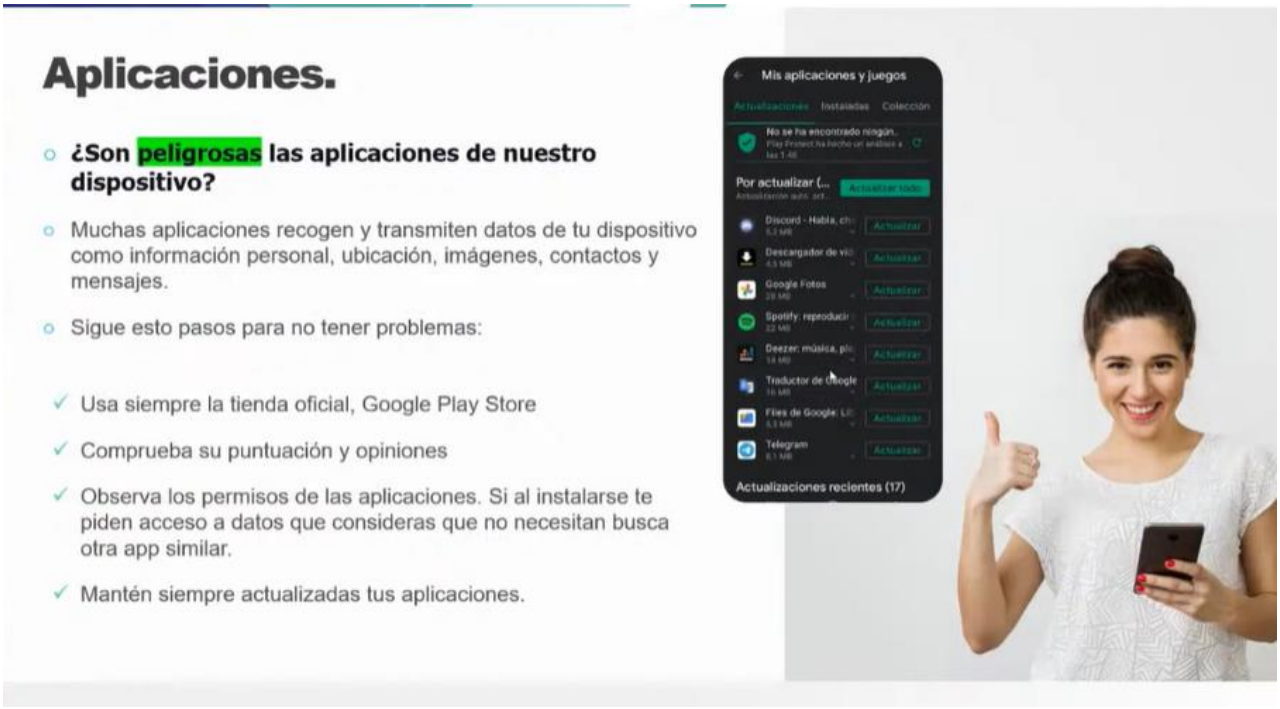


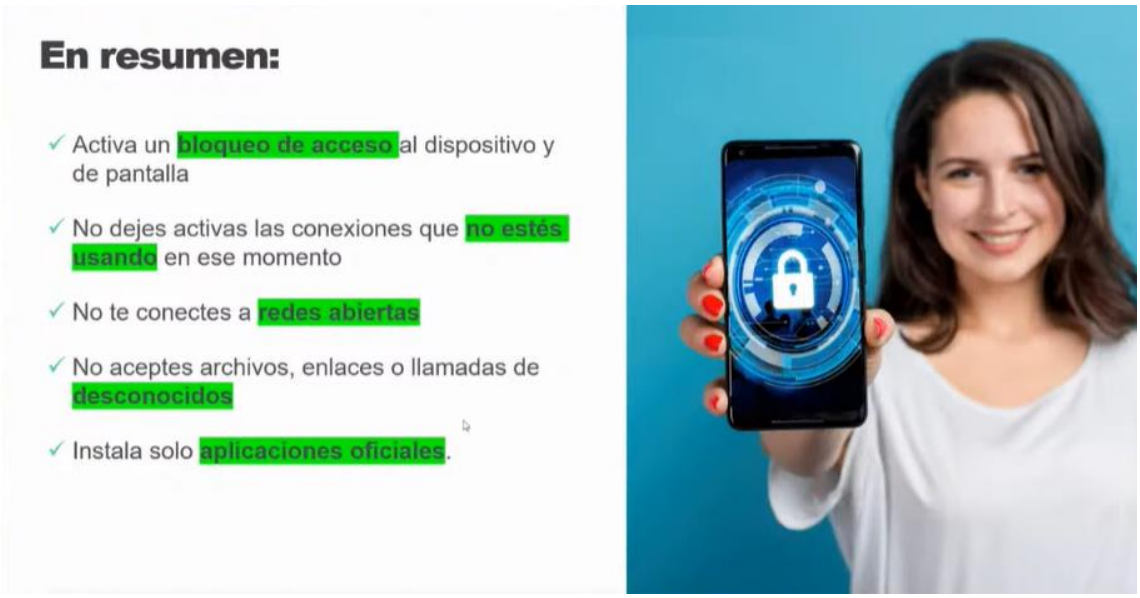
Instalar aplicaciones





Actualizar SIEMPRE las aplicaciones y por supuesto nuestro Sistema Operativo Android





NUESTRO CORREO ELECTRÓNICO

E-mails que no debes abrir o tener cuidado

Hay determinados correos electrónicos que simplemente con echar un vistazo ya sabemos que son peligrosos. Nos muestran algunas señales que nos hacen dudar. Vamos a ver cuáles son las principales.

Direcciones que no conoces

Lo primero a tener en cuenta es cuando recibimos una dirección que no conocemos o ésta es extraña. Esto puede indicarnos que se trata de una estafa o de algún tipo de peligro. No decimos que directamente **borremos el e-mail**, pero sí que se tenga cuidado a la hora de abrirlo e interactuar con él.

Archivos adjuntos

¿Tiene archivos adjuntos ese correo? Si vemos que puede ser peligroso y además tiene **archivos adjuntos** hay que extremar las precauciones. Por supuesto nunca debemos ejecutar o descargar archivos adjuntos si no sabemos con total certeza que es seguro. En caso de que lo hagamos podemos comprometer muy seriamente nuestro equipo.

Asuntos en el mensaje que piden rapidez o urgencia

El asunto del mensaje puede ser la clave para saber si es una estafa o no. Normalmente los **correos electrónicos** que tienen algún peligro detrás suelen utilizar asuntos de mensaje que evocan a la urgencia o rapidez. Por ejemplo nos indican que nuestra cuenta ha sido robada, que tenemos que llevar a cabo una acción para que nuestro equipo no esté en peligro, etc.

Lo que buscan básicamente es llamar la atención. De esta manera picamos en el anzuelo y accedemos a ese correo. Ahora bien, dentro del mismo puede contener algún enlace o archivo adjunto malicioso y afectar a nuestra seguridad.

Piden datos personales

Otro tipo de correo electrónico que recibimos y que puede ser un problema es cuando **piden datos personales**. ¿Nos dicen que rellenemos un formulario donde nos piden datos como nuestro teléfono, DNI, dirección…? Puede tratarse de un engaño para simplemente obtener nuestros datos personales para fines publicitarios o incluso venderlos a terceros. Lo mejor, a no ser que estemos muy seguros de que ese correo no es malicioso, es que nunca interactuemos con ellos.

Traen enlaces sospechosos

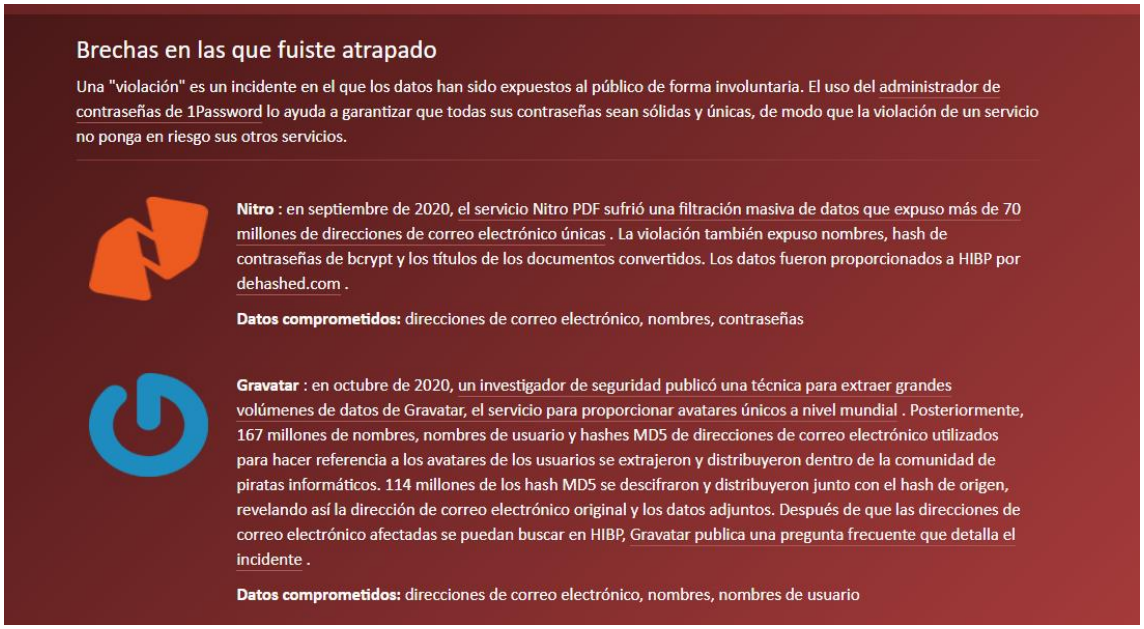
Por supuesto cuando hay un enlace sospechoso lo mejor es ignorar ese correo. Puede tratarse de **un ataque Phishing** que busque que iniciemos sesión en un determinado servicio a través de sus enlaces. En realidad, al poner nuestro usuario o contraseña vamos a enviar la contraseña a un servidor controlado por los atacantes.

Phishing

Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios.

Enlace para comprobar si tu correo electrónico ha sido utilizado de forma fraudulenta

https://haveibeenpwned.com/



Sentido común

Lo último, aunque quizás sea lo más importante, el **sentido común**. Muchos tipos de ataques llegan por descuidos o errores que cometemos los usuarios. Tenemos que mantener el sentido común en todo momento y no cometer errores que puedan afectarnos.

30 apps, que pueden realizar algún cargo a tu cuenta

https://www.larazon.es/tecnologia/20210829/nmaytpzur5espgwvvrwjmagm4a.html

Cargan sobrecostes a los usuarios mediante suscripciones elevadas o compras internas

La compañía de Ciberseguridad Sophos ha descubierto 30 aplicaciones poco éticas dirigidas a los usuarios de móviles iPhone/Androi que buscan cargar sobrecostes a los usuarios mediante suscripciones elevadas o compras internas

Entre las 30 apps se encuentran editores de imágenes, lectores de horóscopos, teléfonos de la suerte o lectores de futuro

Se ha aconsejado a los usuarios una serie de medidas de seguridad para evitar este tipo de software, que pasan por instalar solo aplicaciones de las tiendas oficiales **App Store o Google Play** e incluso en estas plataformas, examinar con cuidado las nuevas o las que se han conocido a través de anuncios.

> Un aspecto importante para los usuarios es que sepan cómo cancelar las suscripciones, ya que no basta con borrar la aplicación del dispositivo, y que sigan las instrucciones de la App Store o Google Play.

Estas son las apps

- Selfie Art – Photo Editor
- Seer App:Face, Horoscope, Palm
- Palmistry Decoder
- Lucky Life – Future Seer
- Life Palmistry – AI Palm & Tag
- Picsjoy-Cartoon Effect Editor
- Aging seer – Faceapp,Horoscope
- Face Aging Scan-AI Age Camera
- Face Reader – Horoscope Secret
- Horoscope Secret
- CIAO – Live Video Chat
- Astro Time & Daily Horoscope
- Video Recorder / Reaction
- Crazy Helium Funny Face Editor
- Banuba: Face Filters & Effects
- QR Code Reader – Scanner
- QR Code Reader & Barcode PRO
- Max Volume Booster
- Face Reading – Horoscope 2020
- Forecast Master 2019
- mSpy Lite Phone Family Tracker
- Fortunescope: Palm Reader 2019

- Zodiac Master Plus – Palm Scan
- WonderKey-Cartoon Avatar Maker
- Avatar Creator – Cartoon Emoji
- iMoji – Cartoon Avatar Emojis
- Life Insight-Palm & Animal Face
- Curiosity Lab-Fun Encyclopedia
- Quick Art: 1-Tap Photo Editor
- Astroline astrology, horoscope
- Celeb Twin – Who you look like
- My Replica – Celebrity Like Me

Web de interés de contenidos de informática:

https://www.andaluciacompromisodigital.org/formacion/

https://www.andaluciacompromisodigital.org/recursos/