117. OnlyFake e iOS Notifications Fingerprinting

una página alojada en la Deep web permite crear documentación gubernamental como tarjetas de identificación carnets de conducir y pasaportes customizables usando Inteligencia artificial y que pueden ser usados para saltarse las verificaciones de servicios como bancos online y exchanges de criptomonedas todo por 10 las notificaciones en iOS permiten a aplicaciones enviar datos de análisis a servicios online que facilitan la de anonimización de usuarios incluso cuando dichas aplicaciones están cerradas y potencialmente sin dejar rastro estamos de vuelta al completo y con noticias frescas como siempre en este nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio es el episodio número nombre y tenemos de vuelta a Don Alexis porros Hola alis Muy cuando vuelvo al podc tierra de hackers ech de menos los ches del señor y estar más cerca de nuestra comunidad que he ido y tal Y me oye Alexis qué la gente ya tenía temor que no que no fueras a volver estaba escondido estaba era tu sombra pero no me veían bien pero ahora soy Ahora estoy de vuelta en en en de toda de una pieza Así que nada eh Yo nada voy a comentar lo que creo que nada ha cambiado respecto a redes sociales durante mi ausencia pero nada nada de hecho lo único que ha cambiado es que ahora sé que se me da muy mal decir esas cosas de hecho creo que en un episodio me olvidé en el otro no recuerdo lo que decía como te dejo a ti esa parte pero así que Dale dale Candela para eso estoy aquí para compenetrar noos querido amigo e Pues nada e comentaros como siempre en cada episodio por si no os acordaba ya os vengo a dar la tabarra de nuevo nos podéis seguir en redes sociales dónde estamos pues en todas en las que creáis que utilizáis eh nos podéis encontrar como tierrade hackers o @ tirad hackers también os podéis suscribir a tierra de hackers en cualquier plataforma de podcast ya sabéis Google podcast Apple podcast Spotify Aunque bueno Spotify está un poco en entredicho creo últimamente y también podéis participar en nuestro canal de discord en con nuestra comunidad donde podéis entrar vía tierrademexico faltar las gracias El mencionar a nuestra familia en patreon una plataforma en la que nos puedes apoyar económicamente desde un eur hasta 10 con diferentes eh beneficios dependiendo de con Cuánto quieras aportar lo más importante a lo que estás aportando a este proyecto a que podamos seguir adelante llevamos ya TR años y pico yendo a por el cuarto y no Sería posible sin todos vosotros Muchísimas gracias tenemos gente que está aportando al máximo desde hace años no sabéis lo que nos enorgullece eso porque querrá decir que estamos haciendo las cosas bien y vamos desde luego a seguir esforzándonos y otra parte esencial los sponsors y monat otro que lleva desde el principio con nosotros y que ya sabéis que es una empresa que comparte los mismos valores que nosotros hacer la seguridad más más accesible y transparente nosotros a través de un podcast y monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles y a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echar un vistazo a su web como os digo siempre monat.com y le podéis enviar el currículum a tirad hackers @mon at.com empezamos con la noticia en el episodio de hace tan solo unos días bueno os traía las tendencias de lo que las empresas más importantes de la industria piensan que va a ocurrir en torno a los vectores de ataque que vamos a ver en 2024 y hacía hincapié en la Inteligencia artificial de hecho hacía una sección solo para eso pues es que no ha pasado ni una semana y ya os traigo la primera noticia de

2024 que combina Inteligencia artificial y cibercrimen a la perfección Y que además ya está generando ingresos para los creadores 404 media publicaba Hace unos días un artículo sobre un nuevo servicio accesible mediante tor ya que está en la de web que se llama only fake only fake es un servicio que te permite crear identificaciones falsas que son perfectas copias de cualquier documento gubernamental como la tarjeta de identidad que todos tenemos y nos nos identifica nuestro país No por ejemplo el dni en España pero no se queda en eso también crear otro tipo de documentos como pasaportes carnes de conducir todo te permite hacer esta herramienta Y sabes por Cuánto por 15 poco más que 10 esto lo sabemos porque los periodistas hicieron la prueba y se generaron un carnet de conducir falso de California os puedo decir que parece totalmente real porque yo tengo uno también ya que viví muchos años en California y es que es igualito de la manera en que funciona Es que este servicio only fake te genera una imagen como si lo hubieras sacado tú una foto al carnet de conducir de hecho en la foto de los periodistas parece que el carnet falso está como encima de una encimera de cocina en plan así con textura de piedra pero he visto otras fotos como si pues los carnés estuvieran encima de una cama o encima de un mueble de una mesa La idea es que muchos servicios online hoy en día hacen verificaciones a través de internet has de enviarles una foto de tu identificación y luego una foto pues normalmente de tu cara no Así es como funcionan muchos bancos y sobre todo páginas donde puedes comprar criptomonedas este servicio brinda una oportunidad perfecta para que la gente barr delincuentes puedan abrir cuentas bancarias o comprar bitcoin con información falsa y estando totalmente verificado con un documento gubernamental todo esto empieza en un canal privado de Telegram donde el creador de este servicio que se hace Llamar John wick publica que La era de la falsificación de documentos de Photoshop ha llegado a su fin Ese es su slogan según él los generadores como é lo llama que ha escrito pueden crear hasta 20.000 documentos al día y se pueden generar partiendo de un ex con la información personal que se quiere Añadir al documento falso es decir tú te haces un Excel con tus columnas nombre apellido fecha de nacimiento dirección cuando caduca el documento la foto eso se lo subes todo y te empieza a generar todos los documentos el periodista empezó poniendo los datos personales que quería usar Y subió en este caso una foto suya personal él comenta que lo hizo así porque no quería utilizar la foto de otra y luego os comento un poquito más sobre esto a partir de eso el siguiente paso es escoger una firma que el servicio va generando automáticamente hasta que encuentres la que te buscas una firma digo como cuando firmas un documento un papel Pues eso lo que hace es coge tu nombre otr veces coge el nombre y el apellido las iniciales y te va generando con Inteligencia artificial diferentes firmas hasta que encuentres por la que te gusta según el creador la red neuronal según él que dice que usa es capaz de crear firmas muy realistas y una vez eliges la firma el sistema se pone a generar el documento elegido en este caso como decía un carnet de conducir de California y en pocos segundos muestra una previsualización al periodista dándole la opción a pagar para poder descargár Sela insisto $ el proceso comenta el periodista que le llevó un total de de 2 minutos Es decir con 2 minutos online subiendo una fotillo que no tiene ni que subirla que lo comento luego y con 15 ya tienes una foto de un documento falso y el resultado son dos archivos una foto del carnet por delante y otra por detrás esto es importante porque hay que destacar que por ejemplo el carnet de conducir californiano por detrás tiene una banda que tiene en codea los datos personales para que se pueda leer con una máquina sabes a veces Pues en el aeropuerto te lo escanean en vez de tener que ellos estar escribiendo todos los datos no y por supuesto la Inteligencia artificial recrea la banda code Ada de manera que contiene los datos también

haciendo todo muy real una pasada la verdad comenta el periodista que el canal de Telegram a veces va poniendo fotos de documentos generados para hacer publicidad el periodista ha visto desde pasaportes australianos hasta tarjetas de identidad de Canadá pasando por garnets de conducir de otros Estados Americanos pues como Arizona ahora mismo según él la herramienta genera documentos de una docena de países y por lo visto incluye España por lo que he visto por ahí una vez con el documento generado en la mano el periodista se propuso testear si era posible efectivamente completar el proceso de verificación de un exchange de criptomonedas que como sabéis en Estados Unidos está sujeto a la ley conocida como kyc lo de know your customer que requiere que toda entidad financiera verifique la identidad de sus clientes para esto usaron el exchange okx porque es uno utilizado a menudo según ellos por delincuentes y que tiende a apcer muchos en documentos judiciales no pensemos que el tema de los exchanges es ahora mismo lo único que dificulta el robo las estafas con criptomonedas porque las criptomonedas no valen de mucho al menos hoy en día Si no puedes convertirlas a dinero real Y es ahí donde entan en juego los exchanges si ahora puedes tener un un exchange con datos falsos y un banco también con datos falsos ya puedes transferir las criptos robadas y cambiarlas a euros o dólares y sacarlas en un cajero o efectuar compras online todo con el anonimato este exchange para su proceso de verificación Pide al periodista sacar una foto de ese carné de su carné Bueno claro en él lo que hace es sacar una foto a la foto que fue generada por on fake es decir la pone la pantalla de su portátil y le saca una foto con su móvil encuadrando por supuesto de manera que parezca una foto real no no que salga la pantalla del portátil no luego le pidió una selfie la cual se hizo Ya que en este caso estaba testeando la parte de aceptación de documentos falsos generados con con Inteligencia artificial pero si hubiese probado con una foto diferente No pues claro tendría que hacer una selfie de otra manera pero eso es todo zas proceso completado y verificación realizada con éxito objetivo cumplido ya estaba dado de alta con identidad verificada según la normativa kyc habiendo usado un documento falso generado con Inteligencia artificial y adquirido la Deep web por 15 El futuro es hoy señores Ahora toca mirar más a fondo qué es lo que ha pasado y es que en realidad por Norma general este tipo de servicios no impl ellos mismos el sistema de verificación de identidades sino que usan alguna empresa externa en el caso de okx no no es una excepción y ellos usan a humio como parte del proceso el periodista contactó a esta empresa y la respuesta fue que ellos solo podían comentar sobre su propia tecnología y no sobre lo que hace luego okx según jio su tecnología es robusta y previene el fraude relacionado con la falsificación de documentación Pues no sé yo la verdad a los hechos me remito el periodista ha podido colarlo Ok por su parte niega las acusaciones de ser permisivo con el cibercrimen y comenta que en el uso de tecnologías de Inteligencia artificial pues es un campo en constante evolución y que hacen todo lo que está en su mano para combatir este nuevo tipo de amenazas bueno Esto es verdad lo que dicen Pero bueno también Es verdad que los documentos judiciales están ahí que los delincuentes tienen una preferencia no por este exchange pero sea como fuere Lo cierto es que el periodista consiguió verificar su cuenta y tenía vía libre para comprar vender e intercambiar monedas con criptomonedas bajo una identidad falsa que ha sido verificada el periodista a cargo de esta investigación se puso en contacto con un experto en la persecución del fraude y le comentó este que efectivamente este tipo de servicios se usan para esto esto de generación de documentos falsos para darse de alta en servicios de compraventa de criptomonedas y bancos muchos están relacionados con el crimen conocido como carding que no es más que el robo de información de tarjetas bancarias pues mediante múltiples métodos como el hackeo de pasarelas de pago tpvs

clonado de tarjetas skimmers instalados en cajeros y bueno muchas que ya técnicas que ya os hemos comentado aquí en tierra de hackers Pues ahora ya tienen este servicio de only fake para conseguir de esas tarjetas de crédito Eh Pues criptomonedas monetizar lasas transferencias a sus cuentas bancarias con identidad falsas vamos que se le ha facilitado la papeleta un montón una de las cuentas de bitcoin asociadas a only fake que es donde recibe pagos en bitcoin contiene ahora mismo $3000 ahora mismo eh que puede ser que hayan movido más dinero pero veamos a 15 el documento estamos hablando de 15 documentos falsos que han sido comprados hasta la fecha como mínimo según John wick el creador de only fake su sistema de creación de documentos falsos puede pasar las verificaciones de servicios como airbnb revolut Kraken wise binance coinbase y y muchos otros más yo os Pongo aquí los que yo conozco hablamos de los principales servicios de banca online de criptomonedas y la web por excelencia de alquilar casas vacacionales una locura indagando Y bueno reflexionando también sobre cómo funcionan estos sistemas de verificación he visto que no solo se basan en la imagen sino también en los metadatos pero fíjate que only fake lo tiene todo pensado y en en la imagen que generan te permiten alterar los metadatos para que parezca una foto hecha con un iPhone y manipulando los datos de GPS para que sea acorde a desde donde la estás subiendo Así que el periodista se puso los metadatos que la foto la hizo con un iPhone 11 y que subía la foto desde Los Ángeles ya que era un carnet de conducir de California vamos que lo tienen todo pensado only fake también te brinda la opción de elegir entre miles de rostros si es que no quieres dar el tuyo y generar uno tú mismo lo curioso es que el claimer que dice que esos rostros no fueron generados por Ai O sea que a saber de dónde los han sacado Parece ser que este proyecto entre comillas por llamarlo de alguna manera empezó hace unos 3 años y solo la parte de redes neuronales según lo que dice el creador que utiliza Les costó hacerlo un año y medio lo crearon metiendo miles y miles de imágenes de documentos gubernamentales reales y claro no es que haya por ahí un repositorio de github con imágenes de documentos de pasaportes y carnes de conducir Así que está claro que algo de crimen ya ya movía el tío pero Espérate que esto no es todo en su canal de Telegram con toda la cara el creador Pide a la comunidad Apoyar el proyecto subiendo más fotos de documentos reales y a poder ser con una definición lo más elevada posible habla de que compraría esos de documentos con una resolución mínima de 10000 dpi ya sabéis cuando utilizáis vuestro escáner en casa no para escanear algo pues ahí la resolución lo más alta posible y que llega a pagar hasta $100 si el documento es estadounidense porque parece ser que tiene una preferencia por ello que tiene sentido menuda visión de negocio tiene el tío muchos servicios de estos empiezan a requerir Realmente si lo pensáis e vídeos en vez de fotos precisamente por razones como estos en las que normalmente te pide Gira la cabeza a la izquierda Gira la cabeza a la derecha escribe yo he visto alguno de escribe eh estos cuatro dígitos en un papel y te haces una foto con eso pero los periodistas flipa con esto comentan que en el propio canal de Telegram ya están haciendo brainstorming y ofrecen una solución yo Esto me quedé flipando resulta que por 45 puedes comprar vídeos de gente haciendo Exactamente eso para ti sujetando Incluso un papel en blanco para que tú puedas sobreponer lo que necesites en postproducción comentan que no saben Cuál es la naturaleza que ha llevado a estas personas a hacer esos vídeos si es que han sido engañadas o o a lo mejor aceptan pagos por ellos sin saber realmente que se está utilizando para verificar cuentas por grupos cibercriminales recordar nadie da nada gratis nadie da duros a peseta si te ofrecen $ por por un vídeo de 10 segundos Mirando a las cámaras y girando girando la cabeza según te dicen será por algo y ese algo pues no es nada Bueno de hecho me trae recuerdos de la gente escaneando ese el Iris con el tema

de de worldcoin querido oyente la próxima vez que vayas a por un café a Starbucks no lo hagas y háztelo en casa con eso ya te has ahorrado los 5 que posiblemente te que posiblemente te puedan pagar por algo así Qué interesante Martín madre mía echaba de menos lo de qué interesante Martín te voy a preguntarlo de Cuántos países pero ya lo has contestado 12 países entre ellos Estados Unidos y España me queda Sí he visto 12 países mencionado los periodistas y según buscaba más he visto por ahí un dni español generado O sea que y vamos que el tío está metiendo más me imagino que se está centrando por el tema eso que decía de que paga hasta $100 por eh pasaporte americanos Bueno cualquier documento americano se estará centrando donde más pueden monetizar entiendo yo que también se está fijando en la población Porque al fin y al cabo es su su potencial clientela no no si te lleva el mismo trabajo hacerte un docum un las redes neurales para un pasaporte español que para uno americano pero Hay muchísimo más americanos que españoles que a lo mejor quieren hacer eso entonces eh Supongo que por ahí van los tiros pero sí sí yo he visto por ahí un dni en un artículo de de otra web que se hacía Eco De esta investigación con un dni Qué bueno y Y cómo cómo han pagado los los periodistas los 15 por bitcoin Ah vale vale iba a decir con su tarjeta con su nombre no no pero ostra a lo mejor estoy pensando el John wick este acepta transferencias bancarias con su iban con su Swift code Y todo porque no no digo porque podría porque se ha hecho un dni y se ha hecho una cuenta falsa de banco entonces en plan para que veas lo bien que funciona esto no no acepto pagos con bitcoin los acepto solo transferencia bancaria no no O sea en este caso era bitcoin pero bueno que ya ya ves menciona revolut que que es yo tengo revolut y y es verdad que no no no tienes una una oficina no lo haces todo online y es verdad que tiene esa verificación a través de de imágenes y todo esto Pero tú la de revolut te la has sacado también con un documento falso o cómo eh No no eso no es nunca nunca jamás si no eh jumio esta empresa de hecho me suena pero a a empresa que que gestiona logs pero no sé si debe haber otra con un nombre similar que se dedique a o ofrecen más servicios o puede que sea una externa pero sí que es verdad que algo que me toca los digo los pies pero lo que me toca es otra cosa e tío las conferencias por ejemplo me acabo de registrar en el Mobile World Congress aquí en Barcelona tío y tienes que subir tu dni tienes que subir una o sea como si estuvieses haciendo un kyc o sea como si estuviese abriendo una cuenta bancaria Pero qué me estás contando o sea Pero qué es esto qué qué pasó con aquello de de me bajo el QR igual que en los conciertos y voy y ya está Qué pasa que porque es diferente esto que ir a un concierto tío y yo he puesto la verificación manual todo manual y y Bueno hasta aquí puedo leer No puedo no puedo decir exactamente qué he hecho Pero bueno tengo que hacer una videollamada con una con un señor o una señora para que esa persona verifique visualmente lo que yo he hecho porque he elegido manual No porque si lo eliges automáticamente entonces utilizan una third party igual que a lo mejor jumio para hacértelo y yo me negué claro eh pero pero aún así tú tenía que subir una foto de mi documento no de mi cara tío es completamente de verdad eh es algo que me pone de una mala leche tío o sea para ir a una conferencia qué me estás contando tío qué me estás contando que no estoy pidiendo No estoy pidiendo un préstamo No estoy pidiendo una hipoteca no estoy abriendo una cuenta bancaria tío que estoy yendo ahí a a que me den camisetas gratis a la conferencia yo flipo tío tenemos que crear aquí un grupo de resistencia de fuerza de de boicotear esto tío es que no puede ser me indigno tío si tenemos oyentes del Mobile World Congress o alguien queé tal Me encantaría tener una conversación con ellos tío de verdad porque es que a lo mejor Oye estoy abierto totalmente a estar equivocado eh Y si estoy equivocado estoy equivocado he aprendido algo más pero quiero que me expliquen A qué viene esto tío A qué a qué viene esta

estos niveles de verificación tío ni que fuera un evento con un peligro de terrorismo de no sé tío no no lo entiendo de verdad no lo entiendo igual te piden También la misma tienen el mismo escrutinio cuando te unes online solo que en persona te imaginas pero yo es que es que me parece increíble tío que o sea tú imagínate de miles y miles y miles de personas que van ahí y evidentemente estas conferencias entre el networking y tal van chupando todo los datos Y compartiéndolas con los vendors que bueno hasta ahí lo puedo entender pero tío ahora tengo que subir fotos de mi pasaporte de mi dni de mi cara sujetando el Pero qué me estás contando t Debería ser gratis entonces la conferencia porque le estás dando tu documento ya te No no ya mira mira me voy a ir a los sponsors no vaya a ser que worldcoin sea sponsor Diamond tío Mira seguro si veo eso ya flipo tí no te extrañe Esto me recuerda también he visto algún algún hablando de nuestra comunidad de discord alguien en discord puso que Hacienda también en España quiere pedir el dni para cuando se saque dinero de un cajero en el en un futuro no muy lejano no sé si leíste eso pero creo haberlo leído No no lo he leído pero tío pero incluso eso que que me parece malo vaya por delante O sea me parece no puede ser pero es que insisto hablo de una maldita conferencia tío de una conferencia o sea compro algo doy mis datos y mi email y ya está y me descargo un es que como en un concierto tío como irme a una fiesta de música electrónica es que no hace falta más qué tiene esto de especial Porque es esto mejor que ir a ver a a Marco Carola tío ahí pinchando tío es que bueno nada ya llevo aquí los oyentes ya deben estar hasta también hasta los pies de mí que llevo aquí creo estoy mirando ahora el el editor de sonido llevo como 7 minutos cabreado ya está ya estoy relajado Gracias Alexis es que Me faltabas ves se me acumulaba la tensión Es que yo saltando un monólogo llevo un mes aquí episodio tras episodio te echaba de menos tío igualmente igualmente echaba de menos ser tu saco de arena mi saco mi saco de arena o mi o mi saco de de boxeo no es justo ese ese es arena duele tío yo no sé a qué gimnasio vas tú pero pero soltar guantazos a un saco de arena de Rocky Balboa que se entrenaba con eso no creo no eso eso le daba le daba puñetazos a chuletones tío no se metía había ahí una vaca muerta colgada tío En el congelador y el pavo se envenenaba tío se envenenaba de hecho así es como hacen el wagi no que le dan masajes no es realmente un boxeador que está ahí dándole que te pegó tal cual se se me ocurría eh comentabas también que al final de la noticia que ofrecía dinero por porque que le apoyen que la apoyen y y que suban imágenes de alta calidad de documentos se me ocurría como hay tantos investigadores dicen que se podría digamos envenenar no a sistemas de Inteligencia artificial alguien algún Buen Samaritano o no sé las fuerzas del orden y eso podrían recabar documentos igual falsos también enviárselos con cierta no sé de cierta forma he visto que hay algún proyecto que se puede utilizar para que una imagen original esté como digamos envenenada o tenga algo como un watermark o alguna historia para que luego las imágenes generadas a través de Inteligencia artificial pues o no salgan bien no salgan lo más realistas realística posibles o bueno qué eso que tengan el el marest te Digamos si se puedan trar o alguna alguna historia así se le podría hacer para un poco charrar El Chiringuito tío me acabas de dar la idea Ah yo había leído un artículo parecido al que dices tú que hace como pequeñas modificaciones lo que había visto es que era para prevenir que se pueda entrenar eh que la Inteligencia artificial se puede utilizar para entrenarse en base a las imágenes tuyas Entonces le añades como esto y como que digamos distrae a la Inteligencia artificial pero tío ya está hackeamos al hacker nos da 100 pavos por un pasaporte español por un pasaporte americano por 15 pavos yo conozco un servicio que me da un pasaporte americano Entonces si le pagamos para que nos genere un pasaporte americano y se lo subimos tío zas 85 pavos ya está tío ya está millonarios aquí sacamos ideas de negocio a punta

pala así se hackea el hacker tío Ya está ya está ahora mismo me pongo a escribir el de python tío venga muy bien Vamos a hacer vamos a crear documentos y a sacar pasta para el podcast claro Pues nada muy buena Martín como siempre la noticia muy interesante nada pasamos pasamos a la siguiente si te parece dale Dale pues Traigo una noticia que va de notificaciones en iOS sé que Martín cubrió una noticia similar no similar sobre el mismo tema eh hace tres episodios pero esta también va sobre notificaciones en iOS eh es algo distinta tiene Ah también un toque de privacidad pero viene los tiros vienen por otra parte no un par de desarrolladores de iOS de aplicaciones para plataformas iOS ha descubierto que aplicaciones populares en el ecosistema de dispositivos móviles de Apple abusan de las notificaciones Push que es como se les conocen para enviar datos de análisis de la aplicación e información del dispositivo a sus servidores remotos Incluso si las aplicaciones no se están ejecutando en tu iPhone estas aplicaciones confirmadas por los investigadores y que han mostrado en un vídeo en YouTube incluyen tiktok Facebook x o Twitter linkedin y Bin aunque esta lista podría incluir muchas más aplicaciones son en en las que se han enfocado comentar brevemente el ciclo de vida de aplicaciones en iOS Pues el ciclo de vida de una aplicación en un iPhone empieza cuando el usuario toca el icono de la aplicación en la pantalla de inicio la aplicación se lanza la interfaz de usuario de la aplicación se muestra en la pantalla y pasa de al estado digamos de primer plano que es la aplicación está activa y recibe la interacción del usuario y realiza sus tareas puede pasar del estado de primer plano a segundo plano si el usuario cambia a otra aplicación lo típico que hace es deslizas tu dedo desde abajo hacia arriba y te sale toda la lista de aplicaciones como en un abanico y eliges otra o bueno de alguna otra forma cambias a otra aplicación o también si se bloquea al dispositivo es cuando las aplicaciones que están corriendo en primer plano la la que tenías abierta pasan a segundo plano la aplicación cuando está en segundo plano se suspende y entra en un estado de bajo consumo de energía Aunque puede realizar tareas limitadas en este modo de segundo plano como actualizaciones del contenido de la propia aplicación o notificaciones y es aquí un poquito lo que voy a comentar en esta noticia y luego llegamos al estado también de cierre no que es cuando el usuario cierra la aplicación manualmente o también automáticamente por parte del sistema operativo iOS puede ser que la aplicación se cierre por falta de memoria o recursos en este caso la aplicación se libera se se elimina de la memoria y se eliminan los los datos temporales que estaba utilizando y finalmente ya tenemos el reinicio no cuando se vuelve a iniciar eh el usuario la toca de nuevo no y vuelve al al estado en en el que se inicia la aplicación el comportamiento del ciclo de vida de aplicaciones en iOS puede variar ligeramente según la versión del sistema operativo y el tipo de aplicación pero normalmente funcionan de esta forma las aplicaciones de iOS no tienen el lujo de ejecutarse en segundo plano por razones principalmente relacionadas con la privacidad y el rendimiento como la duración de la batería que dure lo máximo posible iOS suspende y eventualmente termina cualquier aplicación que no esté activa Así es como está diseñado en iOS pero a partir del iOS 10 que probablemente es principios del 2010 por ahí iOS agregó una nueva función que permite a las aplicaciones personalizar sus notificaciones Push Incluso si no se están ejecutando y voy a comentar un poquito más el modo en segundo plano qué qué pueden hacer las aplicaciones en segundo plano Pues el segundo plano está diseñado para tareas específicas de la aplicación consideradas esenciales digamos que esto algunos ejemplos de esta funcionalidad son aplicaciones de música para continuar reproduciendo el audio o el podcast que estás escuchando ahora mismo también eh temas de ubicación pues rastreador de actividad física Pueden seguir tu ubicación para calcular la distancia y mapear la ruta que Estás siguiendo aplicaciones de

comunicaciones de voz como voz sobre IP pues estas aplicaciones digamos por ejemplo Skype pueden mantener la llamada en curso y también tenemos aplicaciones de noticias que e ya pueden ser de tiempo o de noticias en sí que pueden e Pues eso pueden recibir e recabar obtener tener más información para actualizar la la aplicación en todo momento el uso de apis de las apis son las digamos las funcionalidades del sistema operativo que el sistema operativo ofrece a las aplicaciones Pues cuando las aplicaciones están en segundo plano el desarrollador cuando está desarrollando la aplicación tiene que pedir eh aprobación explícita de las appis las funcionalidades que va a utilizar cuando la aplicación se corra esto sucede eh cuando el desarrollador envía su aplicación a al Apple Store para que sea aprobada pues las apis disponibles en segundo plano son acceso a la red la Api de ubicación reproducción de audio y actualización de contenido un poquito relacionado con lo que con los ejemplos que acabo de comentar y os voy a comentar las apis que no están disponibles en segundo plano no está disponible el acceso a los sensores por ejemplo aplicaciones en segundo plano no pueden acceder a la mayoría de los sensores del dispositivo como la cámara el micrófono o el acelerómetro no sobre todo cámara y micrófono sería te te estarían sería objeto explícito de espionaje tampoco en segundo plano tampoco se permite ejecución de código en segundo plano y tampoco se permite acceso a agenda contactos ni fotos pero sí que en segundo plano se permiten las las notificaciones es decir las aplicaciones pueden recibir notificaciones sobre eventos eh Mediante los típicos banners arriba o las insignias o cuando está en modo el teléfono está bloqueado también muestran un un popup una ventanita con el mensaje y también en segundo plano se permiten tareas digamos últimas tareas de una aplicación para que se pueda cerrar de forma exitosa es decir que por ejemplo si estás redactando un correo electrónico pues puede ser que se le dé un breve periodo de de Gracia digámoslo así a a la aplicación para completar la tarea para es decir cerrar la aplicación de forma correcta para que ese texto no se pierda no sé si alguna vez os ha pasado que que en alguna aplicación la tenéis abierta escribís algo la cerráis luego volvéis a la aplicación y ese texto ya no está no se ha guardado esto también depende de del del desarrollador no si no ha implementado esta funcionalidad de guardar el El Progreso lo que se estaba haciendo de forma segura pues pierdes todo lo que estabas haciendo No pero como digo en segundo plano se le cuando cuando pasa de de primer plano a segundo plano se le permite a las aplicaciones acabar de hacer lo que estaban haciendo básicamente y luego Tenemos también el modo que se llama background app refresh eh o la actualización digamos en segundo plano que no sé si os habéis fijado pero cuando Vais a eh A cada una de las aplicaciones en configuración del iPhone hay una de las opciones normalmente Está hacia abajo del todo de la lista en aplicaciones tenéis no sé acceso a fotos acceso a micrófono acceso a cámara acceso a ubicación y también tenéis el background app refresh que en español no sé cómo sale tengo el móvil en inglés pero debe ser como actualización en segundo plano Y eso es una funcionalidad que se puede eh el usuario puede decidir si la permite o no Y esto es también de nuevo se utiliza aplicaciones la utilizan para por ejemplo aplicación de noticias de Apple la utiliza para cargar historias más nuevas para que estén listas en cuanto abres la aplicación eh aplicaciones de almacenamiento por ejemplo como dropbox pues eh permiten que se sigan enviando los archivos o o que se sigan descargando si se ha iniciado ese proceso aplicaciones de redes sociales pueden ir cargando nuevas actualizaciones para que en cuanto la abras te salgan y no tengas que esperar un tiempo de refresco y bueno aplicaciones del tiempo lo mismo yo De hecho estaba jugando antes un poquito con esto porque lo he visto siempre muchas veces pero nunca me lo he parado a pensar eh de la funcionalidad en Sí por ejemplo en

WhatsApp pues lo he desactivado y cuando he vuelto a abrir la aplicación de WhatsApp me decía activa mejor esta funcionalidad de background app refresh para que Cuando abras WhatsApp eh te salgan todos los mensajes mucho más rápido y no tengas que esperar y todo eso y yo pienso Bueno a mí esto tampoco si me tengo que esperar un par de segundos para que me salgan los mensajes tampoco me me viene de esos segundos Así que lo que he ido haciendo es deshabilitarlo en todas estoy haciendo una prueba digamos a raíz de esta noticia y a ver si si me impacta y si no pues mira Oye si si le puedo dar menos eh si le puedo limitar un poquito el el el uso de de los recursos y y un poquito no sé que que envíen datos a sus servidores a aplicaciones pues eh es lo que he estado haciendo a ver si si si llego a alguna conclusión de que es bueno o malo pues os lo comento Pero bueno al menos quería comentaros un poquito Para qué sirve ese ese modo también para que lo sepáis okay Y ahora entro brevemente a comentar Cómo funcionan las notificaciones Push de Apple que probablemente esto lo comentará Martín en su noticia pero voy a hacer un breve refresco cuando una aplicación recibe una notificación Push iOS despierta dicha aplicación en segundo plano o incluso si está cerrada y se le permite durante un tiempo limitado que se ejecute para personalizar la notificación antes de que esta se presente al usuario esto el caso de uso de de este tiempo de ejecución es para que las aplicaciones por ejemplo un caso muy común es que descifren la carga útil de la notificación por ejemplo estos mensajes como comentaba Martín que a veces Apple y Google pueden espiarnos no a través de eso y no solo eso sino los gobiernos pues algunas aplicaciones si lo hacen bien deberían cifrar estos datos para que nadie pueda espiar y esté cifrado digamos extremo a extremo y la aplicación en Sí descifre este contenido y te lo muestre pues esto sería un caso de uso o también el tema sería de Descargar contenido adicional para enriquecer la notificación antes de que iOS la presente al usuario por ejemplo descargarse alguna imagen de perfil o de alguna de la noticia en sí o de de lo que sea en concreto y Tan pronto como la aplicación termine de personalizar la notificación iOS la termina o sea es como si estaba en segundo plano o estaba cerrada iOS permite digamos la resucita un poco la la trae sería como casi en primer plano y permite que se ejecute Aunque no es en primer plano porque tiene acceso a funcionalidades limitadas ahora os comento el problema es que desarrolladores están aprovechando este método para ejecutar código en segundo plano y enviar datos analíticos desde el dispositivo los datos que se incluyen en en estas en estas peticiones en estos envíos eh Son tiempo de actividad del sistema es decir la la hora actual Y cuánto tiempo lleva encendido el teléfono Configura Regional del idioma del idioma también del teclado no solo de la aplicación o del sistema operativo la memoria disponible el estado de la batería modelo del dispositivo y muchos otros pues estos parámetros estas señales se utilizan comúnmente esto no creo que os venga de nuevo lo hemos mencionado más de una vez en el episodio y que hay empresas decenas de empresas que se dedican a acumular a recopilar esta información y luego la venden no a a gobiernos por ejemplo el caso más sonado no es el tema de de que han habido personas que fueron rastreadas por el tema de abortos y bueno otros temas similares no temas también probablemente se hayan utilizado para seguimiento de de los acontecimientos del 6 de enero en el Capitolio y bueno temas similares ya ya sabéis pero bueno lo que digo es que estas señales que se utilizan comúnmente para la identificación y seguimiento de usuarios en diferentes aplicaciones creadas incluso por diferentes desarrolladores Esto está estrictamente prohibido en iOS y en Ipad os Lo que pasa que de alguna forma estos datos se filtran y y se acaban e recopilando y y se acaban utilizando para de anonimizar a a los usuarios de estos dispositivos el análisis de los investigadores muestra que esta práctica es más común de lo que esperábamos la frecuencia con

la que muchas aplicaciones envían información del dispositivo después de ser activadas por una notificación es sorprendente como ya he mencionado aplicaciones como tiktok x Twitter Facebook y linkedin también esto es muy interesante envían datos al borrar sus notificaciones en el centro de notificaciones es decir cuando recibes una notificación iOS activa la aplicación y le permite correr ciertas funcionalidades limitadas como digo descifrar si los datos están cifrados para que te los pueda mostrar o descargarse algo de internet como una imagen de perfil o algo similar pero no solo eso sino que cuando borras las notificaciones también se permite un tiempo de ejecución y lo aprovechan para enviar datos también a sus servidores esto esto Me fascinó mucho también porque dices el tema de la notificación pensaba que solo estaría limitado a cuando la recibes no a cuando tú eliminas la notificación Así que a partir de ahora Bueno voy a entrar luego más tarde en tema de de prevenciones no pero uno sería no borré nunca las notificaciones porque así no no enviáis más datos de lo si realmente necesitais notificaciones para esa aplicación en cuanto al manejo de datos que se envían las aplicaciones adoptan diferentes enfoques para enviar y almacenar los datos servicios comunes que muchas aplicaciones utilizan son Google analytics y firebase Pero algunas aplicaciones como Facebook utilizan sus propios servicios tiktok utiliza una combinación de Google firebase y sus propios servicios uno se podría preguntar y qué otras razones además de la creación de huellas digitales del usuario porque es principalmente para lo que se utiliza esta información también llamado fingerprinting no que concepto del que hemos hablado más de una vez en el podcast pues qué otras razones aparte del fingerprinting existen para para permitir a los desarrolladores obtener este grado de precisión Por qué se permite el acceso al porcentaje de la batería eh Incluso el el tiempo de arranque el lenguaje Del teclado qué le importa a la aplicación si tengo el teclado en en español o en inglés y cuando estoy escribiendo en la aplicación hay varios temas no que no son tanto relacionados con la privacidad como optimización de la aplicación Pues si la aplicación ve que el nivel de batería está bajando pues puede ajustar el brillo de la pantalla pueden optimizar temas de consumo de menos energía luego También tenemos el tema de la personalización de la experiencia del usuario Pues si e la aplicación le que eh El brillo de la pantalla eh es un nivel u otro lo puede modificar digamos en función de la luz ambiental y también se utiliza para cuando las aplicaciones no funcionan bien no que Hay algún error pues para tener datos de telemetría de de qué estaba haciendo el usuario porque qué ha fallado y mejorar un poco para mejorar la experiencia del usuario pero es eso son estas razones suficientes voy a comentar brevemente el escenario de que voy a poner el vídeo para que lo veáis pero los investigadores muestran cada una de las aplicaciones que han probado Cómo se comportan no cuándo reciben justo después de recibir la notificación y justo después como digo de borrar la notificación que es algo interesante que a mí me ha sorprendido que no sabía que en ese caso en ese momento se podía ejecutar también la aplicación Pues tiktok cuando recibe una notificación envía datos analíticos todo esto se hace vía web vía el protocolo http normalmente competiciones post pero podría enviarse también competiciones get en en el parámetro parámetros de la de la URL Pero bueno Envía una petición vía web a un nombre de de sistema un hostname que se llama Jet gu i18n tiktok.com y envía datos de Eh bueno sistema versión del sistema operativo e tiempo que lleva el teléfono encendido la hora actual la región el identificador el dispositivo entre otros no y luego cuando se borran las notificaciones de tiktok también envían más información pero en este caso lo envían al firebase de Google a este servicio que es un servicio de recopilación de datos no Y en este caso la información es más específica y incluye el momento del tiempo actual y el tiempo que lleva el teléfono encendido luego muestran

Los investigadores en su vídeo el uso el comportamiento de x cuando recibe una notificación pues Envía una petición esto es bastante normal no x cuando recibe una notificación Envía una petición para cargarse la foto de perfil de de la persona del usuario que que ha emitido esta que ha creado esta notificación Ok hasta aquí todo bien pero cuando vas y borras la notificación de X de Twitter la aplicación envía hasta siete peticiones web a diferentes servidores entre ellos de Twitter no de la Api de Twitter de vídeos de Twitter e pero también appg measurement.com connectivity check de Google Google y Crash analytics reports de Google que es un servicio similar o incluso de la familia de firebase de de Google también y esta petición a Crash analytics reports de Google incluye de nuevo el momento de tiempo actual es decir qué hora qué momento es ahora y el tiempo que lleva el dispositivo encendido quiero recordar que Martín cubrió de nuevo hace tres episodios el tema de que las empresas que gestionan y distribuyen notificaciones a dispositivos móviles tanto Apple como Google podrían espiar si quieren dichas notificaciones y potencialmente abusar de nuestra privacidad por ejemplo identificarnos no incluso los gobiernos Okay esto lo entendimos Pero al menos a mí yo lo que pensaba es que esto se quedaba en casa no digamos es decir que solo Apple podía ha notificaciones de dispositivos de iOS y Google de dispositivos de Android Y esto es así eh Cuando digo que pueden ver notificación es así lo único que como se envían datos de analíticas a a distintos servidores en este caso tanto x como tiktok envían datos a Google pues vemos Que aplicaciones en iOS de distintos desarrolladores que utilizan esta una plataforma en común en este caso analíticas de Google en este caso no solo Apple puede ver las notificaciones y de anonimizar digamos identificar los usuarios en recopilando datos de diferentes aplicaciones sino que ahora sabemos que también Google podría identificarnos en distintas aplicaciones abusando de esta información analítica que se envía a servidores de firebase de Google porque incluye como digo eh la se puede hacer se puede determinar eh cuánto tiempo lleva el teléfono encendido y la hora actual Entonces se puede determinar cuándo el teléfono se encendió Este es un indicador que es bastante fiable No solo ese sino que si se combina con el tema de nivel de batería y espacio disponible en el dispositivo pues ya tienes una triada que es bastante fiable para de anonimizar a a usuarios en base a distintas aplicaciones y esto todo lo tiene Google al menos las aplicaciones que utilizan los servicios de de datos analíticos de Google luego brevemente comento que Facebook cuando recibe una notificación eh lo mismo envía eh la la hora actual Y cuánto tiempo lleva el dispositivo encendido esto lo envía a graph.facebook.com Así que se queda un poquito en la propia empresa y cuando se borra la notificación también se envía eh otra otra petición pero en este caso a www.facebook.com con información sobre el iPhone en el caso de linkedin cuando recibe una información se envían datos lo típico no versión del sistema operativo eh la franja horaria el tipo de dispositivo el idioma y similares a www.linkedin.com es solo una única petición y cuando se borra la notificación la app de linkedin Envía una docena de peticiones eh con datos más analíticos a de nuevo el mismo sitio www.linkedin.com es decir que linkedin recolecta demasiados datos que Probablemente sean innecesarios y finalmente se Comenta también el caso de Bing Bueno cuando recibe una notificación Envía una petición con datos analíticos del dispositivo a un sitio suyo gateway.bacb.com respuesta es que sí no sé si os acordáis del episodio 104 en el que unos investigadores comentaban el potencial ataque del modo avión falso en el que una aplicación podría mostrar que el teléfono móvil está en modo avión cuando en realidad el teléfono aún puede utilizar la red de datos móviles sin que el usuario se dé cuenta pues del mismo modo las aplicaciones en iOS podrían elegir descartar silenciosamente las notificaciones Push sin que el usuario las vea lo que les permite realizar un seguimiento del dispositivo y del usuario sin ser

notadas de esta manera la aplicación puede recopilar información del dispositivo o realizar otras acciones sin que el usuario sea consciente de ello este tipo de comportamiento es preocupante desde el punto de vista de la privacidad y puede violar completamente las políticas de Apple si se utiliza para realizar actividades no autorizadas O maliciosas el tema es que parece que es depende de la aplicación en Sí si quiere mostrarte la notificación o no esto Me parece muy muy interesante porque estas aplicaciones como digo podrían recibir una notificación No mostrártela pero ejecutar lo que tengan que ejecutar y enviar datos analíticos a a su digamos a su a sus servidores Eh Esto sucede de forma normal obviamente cuando la aplicación está en primer plan no no pero muchas veces cambias de aplicación y cuando está en segundo plano si se Ha desactivado Eh Pues no te no pueden seguir enviando datos analíticos para para un poquito seguirte pero en este caso si hay algún servicio digamos que se vuelve malicioso y está enviando notificaciones sin parar no sé digamos a una determinada frecuencia una vez cada minuto que esto lo podría modificar en cualquier momento pues la aplicación se despierta se despierta es Digamos como no sé si los que hacen un poco más de red teaming sería como un bicon enviarle un bicon a la aplicación decirle Oye estás viva ejecútese cute algo en concreto Bueno sí podría ejecutar lo que lo que se le pida pero lo más preocupante es que envía información sobre el dispositivo y sobre sobre el usuario en Sí o sea es una forma digamos de espionaje en seguimiento constante no solo temas de problemática de privacidad planteáis sino también un problema de consumo de datos Porque hay usuarios de teléfonos móviles que tienen tarifas que incluyen una cantidad de datos máxima que pueden descargarse o subir y después de la cual su velocidad se reduce drásticamente esto eh No sé si lo habéis experimentado yo lo he experimentado sobre todo cuando voy a otros países en roaming que tengo una tarifa que llegas a no sé 5 gbas y después te baja la velocidad a adsl de de hace 10 años a 256 kbits por segundo y me va todo super lento Así que esto sería una forma en plan de de dejarle a algunos usuarios eh de negarle el servicio de celular no incluso puede ser que algunos se queden sin acceso no sé en algún país No sé si yo creo que igual hace años esto igual se hacía pero yo creo que igual ahora ya no pero igual puede ser que algún país cuando llegues a un cierto límite de datos descargados o subidos ya no tengas Incluso en internet Pero bueno el tema es hombre eso sí sobre todo si estás en el extranjero el tema del roing que probablemente tienes un límite porque si no te puede salir un pastón Oh mira pues se me ocurre que incluso para alguien para alguien hacer la factura más larga También Claro claro claro porque llega un momento en que como no tengas un límite o sea es que una de dos si tienes el límite te quedas sin internet si no lo tienes te quedas sin dinero tú eliges choose poison el tema nada la conclusión de esto es que aplicaciones móviles en iOS echar las notificaciones para ejecutarse digamos en segundo plano obviamente como digo con funciones limitadas no pueden acceder a las fotos al micrófono y temas similares ya sería eso muy obvio de de abuso a privacidad no Y esto al menos Apple lo ha restringido pero sí que pueden enviar ciertos datos como digo de de cuánto tiempo lleva el teléfono encendido eh Y si se envían a ciertos servicios como Google pues Google luego podría también abusar de todo eso y intentar de anonimizar a las personas son datos que no son necesarios para el uso normal de una aplicación y que como digo pueden ser abusados contra nuestra privacidad Y qué podemos hacer al respecto queridos oyentes pues lo primero de todo Y supongo que alguno ya lo está pensando un poco igual viene Obvio o igual no pero el tema de Deshabilitar las notificaciones para prevenir que una aplicación haga esto eh se pueden desactivar las notificaciones de dicha aplicación por completo comentar que establecer alertas de notificación de sonidos o insignias no es suficiente e se tiene que eliminar completamente las notificaciones es

decir hay que ir a notificaciones o a la app en concreto y desactivarlo las insignias estas para los que no sepan eh Son las son ese ese círculo rojo en la parte superior derecha de la aplicación que contiene un numerito con la cantidad de notificaciones pues aunque dejes esto eh y y elimines el banner no se tiene que eliminar completamente para que no se puedan ejecutar cuando recibe una notificación Porque si se desactivan las notificaciones Entonces el sistema operativo iOS no va a permitir que la aplicación se ejecute porque no se recibe ninguna notificación un dato bueno algo algo que nos puede dar esperanza es que a partir de la primavera digamos de este año Debería ser eh Cuándo es en marzo no el 21 de Marzo a partir del 21 de Marzo pues Apple va a requerir que los desarrolladores declaren las razones y los motivos para usar las apis que devuelven señales de dispositivo únicas como comúnmente utilizadas para el fingerprinting todo esto que he mencionado es decir los desarrolladores tienen que justificar Por qué quieren tener acceso al al tiempo que lleva el teléfono encendido Por qué quieren tener acceso a al idioma específico que esté en ese momento utilizándose en el teclado el la franja horaria el Time zone el lenguaje del sistema operativo todo eso van a tener que justificarlo y si no se proporciona una justificación que esto depende de Apple no que apruebe no que le parezca Apple buena o no pues estas aplicaciones no van a ser aceptadas por el app Store y no se van a poder descargar Así que es algo que han han publicado eh como parte de su documentación de desarrolladores así que bueno es algo algo bueno para para nosotros para los usuarios para que paren de de identificarnos y de anonimizar noos otra idea sería bloquear estos dominios involucrados en las notificaciones por ejemplo se podría utilizar eh servidores de dns o cacharros como un p Hole no para para prevenir esto y Añadir estas urls estos dominios bloquearlos para que no se puedan cargar para que nos envíen estas notificaciones con estas peticiones a raíz de una notificación recibida aunque esto requiere un poquito juego de El gato y el ratón No porque si si ven los los desarrolladores los dueños de estos servidores que nos las aplicaciones están recibiendo Endo están enviando menos datos de lo normal van a ver que algo está sucediendo igual pueden cambiar estas urls es decir que los usuarios tienen que estar un poco Ahí analizando si cambian estas urls un poco se puede hacer pero hay que estar ahí investigá constantemente la otra opción sería instalando Bueno una sería haciendo un jailbreak del teléfono Entonces ya se tiene más control sobre los servidores dns que se utiliza pero la otra también he visto ahora no recuerdo el nombre pero hayuna creo que es de pago que también permite un poquito eh Modificar el dns O al menos eh Por aplicación se puede hacer un poco de Proxy y modificar digamos bloquear básicamente Al fin y al cabo las urls a las que se accede por cada una de estas aplicaciones Ahí os lo dejo un poquito más de concienciación sobre el tema de de por dónde vienen a veces a a recolectar nuestros datos de uso de aplicaciones y cómo nos pueden de anonimizar y un poco para que sepáis también Cómo prevenir Desactivar notificaciones y tema de dns bloqueo de de estas urls Pues como siempre muy útil para nuestros oyentes en este caso un poco más de aquello de los sedientas que lle pueden llegar a ser las aplicaciones de que tenemos instaladas en los móviles si te acuerdas yo siempre menciono aquello de Oye utiliza las aplicaciones en vez de las aplicaciones quiero decir la versión web y pongo siempre como ejemplo los linkedin que es una de esas y aparte la mencionaste tú HM yo simplemente ya estoy logueado en mi navegador del móvil la interfaz es exactamente la misma que la aplicación y hoy en día con los nuevos móviles tampoco se nota ahí como sabes a veces Pues antes el navegador va un pelín más lento no es tan no tiene ese esa usabilidad o sabes que vaya tan fina como la aplicación pero vamos no se nota nada Y más si no es un juego sabes que más te dan linkedin si tienes un versión web que tengas un nanosegundo de diferencia a la hora de

procesar la la petición con todo esto decir las versiones web la ventaja que tienen es eso que se recolecta muchísimas menos métricas pero es que ahora tú con tu noticia le has añadido ese siguiente nivel que ya es que aunque no se esté ejecutando la aplicación está recolectando información Igualmente algo que no sucedería si utilizar la versión web por tanto tu objetivo querido oyente es tener la mínimas aplicaciones instaladas en el móvil sin dejar de tener la funcionalidad que necesitas por supuesto correcto mínimas o si tienes alguna incluso que es mínima y no necesitas notificaciones porque no es nada urgente pues Desactiva las notificaciones y es a a mí lo que me ha sorprendido sobre todo es que pueden pueden recibir notificaciones y no mostrártela O sea te están decepcionando como usuario y están ejecutando su código en segundo plano as que con cuidado queridos oyentes Sí sí sí desde luego yo en general tengo todas las notificaciones des activades primero porque distrae un montón eso también y segundo porque si te paras a pensar yo no necesito saber cada WhatsApp que me llega O sea no es una información que necesita y en tiempo real aparte que va me distraía un montón que yo soy una persona que se distrae muchísimo Entonces es que está intentando pensar ahora qué aplicaciones tengo que mente me llega una notif Pues el email y creo que el email lo tengo solo para ciertos con ciertas reglas de Oye si me llega de tal persona o es del email de mi propia empresa Pues sí porque a mis clientes les quiero contestar al momento pero vamos que lo tengo muy muy a raj tabla eso y mira pues otra razón más para motivarnos aunque sea solo por aquello de que nos distraiga menos y miremos menos el móvil ahora tenemos una motivación más la la del banco para que te digan si alguien ha intentado usar un documento de del only fake sí sí sí sí sí justo que nunca nunca se sabe Bueno pues eh siempre siempre curiosa la noticia muy útil y yo creo que con eso que los deberes que le hemos hecho a los oyentes desinstala las aplicaciones que tú veas Pruébalo como decías tú simplemente bueno prueba a desinstalarte Pues empieza por linkedin que a mí me va muy bien Te logeas y miras y dentro de una semana evalúas eh Y si dentro de una semana ves que que no que no va Tan bien que necesitas aquello tal Bueno pues te la vuelves a instalar Y hac eso pues con todas las aplicaciones y así ya está y luego ya ya seguro que acabas con menos aplicaciones de las que pensabas que que ibas a acabar te lo garantizo y hasta aquí Hemos llegado querido oyente Muchas gracias por quedaros hasta el final Como siempre nos despedimos pidiendo que compartáis el podcast con cualquier persona que creáis que le pueda interesar algo así muchísimas gracias por apoyarnos por escucharnos por seguirnos por darle a like por dejarnos comentarios y todo eso Muchas gracias por escucharnos otro episodio más y por estar ahí otro comienzo de año más queridos oyentes y nada nos escuchamos en el próximo episodio Adiós adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de haers