Cuáles son las previsiones de la industria para 2024 en cuanto a ciberamenazas va la Inteligencia artificial acabar con nosotros qué ha sido lo más destacable de 2023 todo esto y más en un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 2 de febrero de 2024 es el episodio número 116 yo soy Martín vigo y vuelvo a estar solito y desamparado ante vosotros pero más a gusto que en brazos con la buena compañía que me dais Alexis se unirá en el siguiente Cómo estáis eh tardado un poquito más en publicar este episodio porque enero ha sido una auténtica locura pero aquí estamos y lo prometido es teuda tenemos un episodio donde cubriremos todos los detalles sobre lo que va a acontecer teóricamente en 2024 Pero antes de nada sabéis que nos podéis contactar en el email podcast @tia la redes sociales Instagram Twitter eh Facebook linkedin lo que queráis nos buscáis como tierra de hackers y en todas las plataformas de podcasting Así que si no estáis suscritos acordaros de suscribiros y también tenemos un canal de YouTube y También aprovecho a darle las gracias a nuestros mecenas de patreon que sin ellos esto no Sería posible si quieres eh tener ciertos beneficios si quieres tener una pegatina oficial de tierra de hackers si quieres tener acceso al podcast sin publicidad vete a patreon y apóyanos que hay varias maneras de hacerlo y esta semana le queremos dar las gracias a uno nuevo a transnor que se ha unido a nuestra familia de patreon y además tiene canal exclusivo a nuestro acceso exclusivo a nuestro canal de discord y le damos las gracias También a nuestros sponsors como siempre a mona una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y mon con una 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 a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com os lo dejo en las notas del episodio y ahí le podéis mandar vuestro currículum por ejemplo a tierrade hackers @m.com y yo creo que empezamos ya como decía íamos el año con un episodio sobre lo que se nos avecina este mismo año o al menos lo que los expertos y la industria en general prevé que va a suceder en 2024 en cuanto a ciberseguridad nos centraremos específicamente en las amenazas productos o infraestructura más probable de ser atacada y nuevos campos de investigación el año pasado había escogido a Kaspersky y su informe para hablar de los trends de este año que acaba de terminar de 2023 y para cambiar pues busque nuevas Fuentes y predicciones de otras empresas importantes y por supuesto con reputación creo que voy a hacer un popurr de de previsiones de trends porque así la noticia será más completa no hablaremos solo de lo que pasará sino también de lo que pasó Qué fue lo más destacable de 2023 Creo que vale también la pena cubrirlo no asemos global del año anterior y del año que viene ahora que estamos justo entre ambos No ahora mismo empecemos por lo que nos cuenta Google en este caso que evidentemente tiene muchísima visibilidad sobre todo lo que sucede en internet dada su apabullante presencia no concretamente el equipo de Google Cloud ha publicado un extenso reporte con sus predicciones para 2024 y vamos a desglosarlo a continuación ya sabéis que lo tenéis las notas del episodio como siempre por si queréis leerlo en detalle por vuestra cuenta cómo no empiezan con la Inteligencia artificial y predicen que el fishing se va a mejorar profesionalizar pero sobre todo va a ser muy escalable normalmente estamos acostumbrados a emails falsos con faltas de ortografía con un contexto muy pobre y con una interacción casi nula si por ejemplo llegásemos a contestar al mail No gracias a la Inteligencia artificial generativa y los llms vamos a ver cómo Esto va a cambiar en 2024 se hará uso de esta tecnología para crear campañas de fishing no solo por email sino también por SMS e incluso por voz mucho más realistas y mucho más profesionales además se automatizará la respuestas en caso de que una víctima caiga en El engaño por tanto ya no se trata de

automatizar el envío del email sino el contestarlo para llegar a la víctima hasta el punto de que esté Pues a punto de pagar o lo que sea que sea la estafa pero Google también avisa que se empezará a incluir imágenes y vídeos falsos para dar más credibilidad lo cual tendrá el efecto contrario Esto me pareció muy curioso en el que el público en general empezará a ser sospechoso de todo dificultando la tarea de empresas y gobiernos que legítimamente quieren contactar con la ciudadanía a través de medios electrónicos esto como digo es curioso llegará un punto en el que ya no nos fiar remos de nada y pasaremos de ser muy poco precavidos a demasiado precavidos es una cuestión interesante ya yo dedico mucha parte de mi tiempo a educar al público en torno a los peligros de internet lo cual por supuesto incluye el fishing y por supuesto incluyo en el material didáctico todo esto de la Inteligencia artificial llegará un momento en lo que hago lo que estoy haciendo con esto de avisar que sea contraproducente pondré al público a tal nivel de alerta que el remedio se puede considerar peor que la enfermedad el tiempo lo dirá pero está claro que enseñar al público a sospechar de todo como solíamos venir haciendo todos en la industria hasta ahora puede que al final no sea la mejor metodología quizá deberíamos cambiar el paradigma a tener más bien sentido común más que ser escéptico y ya qué opináis vosotros queridos oyentes seguimos con el reporte de Google de lo siguiente que hablan para 2024 es lo que ellos denominan the big Four los los cuatro grandes Así es como Google Define a China Rusia Corea del Norte e Irán el grupo de países que esperan que esté más activo en cuanto a ciberataques en 2024 de China destaca Google que seguirá haciendo campañas centradas en preservar el secretismo reducir la capacidad de detección de los adversarios y obstaculizar los esfuerzos de atribución de los ataques ahí es nada eh pero es que además considera que china va a seguir invirtiendo en la capacitación no solo de militares sino de civiles aquello que hablamos mucho de los grupos de apt que están esponsorizar a cabo ataques disruptivos y destructivos que apoyen los objetivos estratégicos nacionales es decir del del gobierno chino el párrafo acaba diciendo que china puede llegar a afectar a la vida cotidiana de ciudadanos de todo el mundo infraestructura crítica Y su seguridad O sea que ya no solo van contra empresas sino que según Google nosotros gente de a pie también vamos a sufrir las consecuencias bastante miedito la verdad de Rusia comentan que se seguirán centrando en el conflicto bélico con Ucrania y que dedicarán la mayoría de su esfuerzo a operaciones de obtención de inteligencia fuera de sus fronteras atacando a objetivos gubernamentales de defensa energ y organizaciones sin ánimo de lucro Bueno un poco en la línea no en cuanto a Corea del Norte Pues tampoco hay mucha sorpresa se seguirán centrando Eso sí con más empeño según Google en el robo de dinero y criptomonedas para seguir costeando su programa nuclear quién diría que que todo el mundo está pagando como un impuesto revolucionario a Corea del Norte para que siga creando bombas nucleares pero pero que es así se centran mucho en el robo de criptomonedas comentan también que han visto más actividad por parte de Corea del Norte relacionada con ataques a cadenas de suministro aquello del supply Chain Attack Por tanto la seguridad de las empresas ya no solo depende de ellos mismos ya no solo tenemos que convencer a las empresas que empiecen a invertir en seguridad para ellos mismos sino sus colaboradores y partners también Y por último nos queda Irán debido a la situación pues candente no en Oriente medio con la guerra entre Israel y Palestina Irán se centrará en el espionaje sobre todo a grupos en contra del propio gobierno también por supuesto y Aparentemente en colaboración con grupos apt libaneses y palestinos Irán va a poner el foco en atacar a Israel que según Google presenta cada vez una amenaza más grande contra el país este tipo de de apts de otros países árabes Así que parece que ambas guerras según Google van a seguir para adelante y por supuesto con un énfasis bastante importante en el la parte cíber el reporte cubre también los tipos de vulnerabilidades que más se esperan ver en 2024 y os voy a mencionar algunas interesantes Pues que para mí

que he elegido cero days Pues yo no sabía esto pero resulta que en 2023 o sea 2023 ostent el récord del año con más cer days utilizados en ataques cibernéticos y se espera que 2024 marque un nuevo récord Por qué cero days Pues porque las empresas que desarrollan software de protección contra ciberataques pues son cada vez mejores detectando fishing y malware y el interés de grupos avanzados de ciberdelincuentes es cada vez más prolongar el acceso a la red interna es decir una vez te comprometo no hago ya lo que sea que quiero hacer robar datos cifrar lo que sea y me piro No no quiero espionaje quiero inteligencia entonces lo que se está viendo es un Trend en el que los apts comprometen las redes y se quedan ahí como una célula durmiente por tanto el uso de vulnerabilidades desconocidas hace que puedan estar infiltrados mucho más tiempo lo que les da más margen como decía para obtener inteligencia ya que explotan vulnerabilidades que no no se conocen todavía otra de las cosas que mencionan son los ataques contra las elecciones estadounidenses este año hay elecciones generales en el país y como vimos en 2016 y en 2020 este año no va a ser una excepción en cuanto a ataques por parte de Irán Rusia y China para influenciar el resultado electoral en las elecciones estadounidenses Google también prevé para 2024 a ataques contra infraestructura aeroespacial este me sorprendió pero resulta que los avances de internet satelital Pues gracias a empresas como starlink y la ayuda de este tipo de tecnología para comunicaciones durante conflictos bélicos Google espera ver el despliegue de toda la capacidad tecnológica de grupos de ciberdelincuentes ampliando el espectro de sus ataques al máximo para incluir satélites ya hemos visto como en el durante el principio del conflicto de Ucrania Pues elon musk dijo que enviaba satélites para poder dar cobertura de internet a la gente en Ucrania mientras Rusia estaba intentando destrozar toda la infraestructura Entonces al tener conexión satelital pues Incluso en las zonas más remotas los los militares todavía podían coordinarse pues entiende Google que vamos a ver ataques en en la zona aeroespacial Por así decirlo para intentar Eh pues prevenir en zona de guerra Pues que haya ningún tipo de comunicación posible siguiente espionaje mediante bonnets durmientes otra predicción bastante curiosa cuando hablamos en de borets no automáticamente pensamos en ataques de denegación de servicio a escala aquello de pues controlo miles y miles de ordenadores Y de repente te mando mando a todos a tu web y te la tiro pero Google comenta que 2024 no solo Seguiremos viendo como ciberdelincuentes van a comprometer dispositivos iot y máquinas anticuadas a gran escala para crear sus botnets sino que lo usarán de manera más encubierta Y sin ninguna prisa dicen para qué Para el espionaje global ya no van a tanto a comprometer dispositivos iot Para tenerlos ahí y lanzar un ataque sino para recolectar información recordemos que las bonet se suele hablar de millones de de dispositivos si tú tienes control sobre cámaras sobre routers sobre no sé qué otros tipos de dispositivos iot Pues no sé sensores Pues ahí hay mucha información que se está procesando Pues empieza a verse un valor de en vez de utilizar estas bonet para tirar servicios que sea para ex filtrar y almacenar información e inteligencia por último la resurrección de vectores de ataques anticuados ole como ejemplo Google habla de un blogpost de un investigador que escribió en 2012 sobre Bueno una técnica para implementar cifrado sin tener que utilizar las apis por defecto del sistema operativo pues comentan que han observado que Esta técnica explicada como digo en 2012 y que pasó totalmente desapercibida se ha popularizado en malware a partir de finales de 2022 es decir plantéate el típico malware ransomware que te cifra la información pues hay mucho mucha detección y edrs y todo esto que ya monitorizan el uso de ciertas apis por ejemplo en Windows que se utilizan para el cifrado de datos Entonces eso pues puede ser una indicación de Oye este ejecutable este binario está utilizando estas apis que se suelen utilizar para cifrar lo cual me hace sospechar que podría utilizarse para cifrado Pues ahora están viendo que se utiliza una tecnica que se explicó en 2012 en el blog de un tío en el que se puede hacer cifrado si teno que utilizar esas

apis comentan también lo mismo con una técnica antim máquinas virtuales ya sabéis donde se suele ejecutar malware para analizarlo que se explica en un libro de malware publicado también en 2012 y que se empieza a ver implementado en muestras de malware recientes porque la industria al no ver estas técnicas explicadas en 2012 en su día en malware pues nunca implementaron detecciones Entonces esto muy curioso básicamente lo que os estoy diciendo es que la gente o sea los cibercriminales están yendo a técnicas explicadas hace muchos años Que nunca se llegaron a utilizar por tanto los los creadores de software de protección nunca llegaron a implementar detecciones en torno a esas técnicas porque nadie las llegó a meter en malware y han visto que es perfecto para bypassear saltarse o no ser detectados en malware 10 años desp después me parece una técnica muy buena en fin ya vemos que Google Dear un 2024 bastante Movidito y como digo tenéis más detalles en el propio reporte si os habéis quedado con ganas de de ver más pero no quiero quedarme aquí 2023 y duda 2024 fue es y será los años de la Inteligencia artificial y esto es un dato que no pasa desapercibido para mí así que decidí previsiones específicas sobre la Inteligencia artificial para 2024 en cuanto a ciberataques y buscando Me encontré con la opinión de un experto mundialmente reconocido el mismísimo miko hipon que además tuve el placer de conocer y charlar unas horas con él en un evento organizado por europol en Madrid el año pasado Pues según mico Este es el top cinco de los problemas de seguridad derivados de algún modo del mundo de la Inteligencia artificial que nos vamos a encontrar en 2024 primero por supuesto Deep fakes Un conocido ya desde hace un par de años pero que ha visto una evolución en su calidad y muy significativa hasta el punto de que se está acercando a que sea difícil distinguir Qué es real y Qué es falso en 2024 esto seguirá evolucionando y nos acercaremos aún más a ese punto tan peligroso men que según un estudio de una empresa londinense en 2023 los ataques basados en Deep fakes aumentaron un 3000 imaginaros lo que vendrá en 2024 Además está también la facilidad la facilidad con la que se puede crear y que lleva a cabo todo o sea incrementa el espectro del perfil del cibercriminal porque tenemos desde gobiernos creando fakes de zelensky declarando la rición la rendición de Ucrania hasta chavales haciendo vídeos de Mr beast ofreciendo iphones gratis supuestamente claro los Deep fakes serán cada vez no solo más reales sino más fáciles de generar una combinación explosiva y Qué podemos hacer para defendernos pues por ejemplo mico sugiere el clásico uso de una palabra clave suena un un poco ridículo quizás a día de hoy pero la realidad es que no es descabellado pensar que a nuestros padres les puede llegar un vídeo por WhatsApp de nosotros pidiéndole dinero típico que te haces un vídeo oye papá Mira estoy aquí no sé qué me puedes enviar un bizum de tal a este número que perdí mi móvil y tal Por tanto acordar entre familiares el uso de una palabra clave y secreta que se tiene acusar en una situación en la que se pide algo urgente o se se notifica de algún tipo de traje pues es algo muy a tener en cuenta y sabéis a lo que me refiero No pues Oye si algún día estás en peligro tal eh o yo que sé te voy a hacer la pregunta de dónde yo que sé dónde pasamos las vacaciones del 89 o Quiero que digas la palabra clave banana o lo que sea no a eso se refiere insisto suena muy peliculero pero es que es tan fácil hacer de Face y cada vez va eh más realistas Y si ya estamos viendo estafas telefónicas donde te llaman y supuestamente han secuestrado a tu hija pues imaginaros si ahora a tus padres les llega un vídeo tuyo pidiéndole dinero de manera casual siguiente tenemos lo que miko denomina como Deep scams traducido como estafas profundas explica que bueno la parte de Deep como en Deep fakes y aquí en Deep scams representa digamos la escala no que que puede escalar que se puede hacer de manera biva digo y a diferencia de Deep fakes Deep scams no implica material multimedia como audio vídeo como ejemplo brinda el famoso documental de Netflix del tindler tinder swindler que Bueno la verdad no supongo que el título en en español será diferente Pero es este del tío que por tinder eh Por si no lo habéis visto aún

ya estáis tardando Eh pues es un estafador del amor que en gatusa y enamora mujeres hasta bueno ganarse su plena confianza y luego les empieza a pedir dinero por por sufrir algún tipo de accidente y lo va pidiendo más y más y más hasta dejarle sin ahorros mico plantea que el uso de llms hubiese hecho que este estafador pudiera estafar a muchísimas más mujeres ya que no tendría que ir contestando manualmente a cada una recordar que es una inversión de tiempo el estar con varias mujeres a la vez contestando a WhatsApp a mensajes Pues sabes ofreciendo cariño Pues haciendo que se enamoren Pues si tú ahora puedes utilizar un chat gpt que conteste por ti de repente en vez de de estar engatusado a cuatro mujeres a la vez lo estás haciendo con 15 o con 20 podría programar la Inteligencia artificial para continuar conversaciones por mensajes Pues en un tono amoroso y cariñoso automatizando así por lo que decía la parte del trabajo y dejándola é centrarse digamos en el punto donde ya llega el momento de estafar a la víctima otra estafa que menciona son las publicaciones falsas en airbnb que hasta día de hoy yo esto no lo sabía usan imágenes de otras reales y que es fácilmente bueno en principio detectable con una búsqueda inversa de fotos en un anuncio yo la verdad no estaba al tanto de este tipo de estafa pero básicamente la gente pone en herv envía anuncios de casas cogiendo fotos de otras para que pague es una reserva y se quedan con el dinero lo que Comenta mico es que con tecnologías como me Journey stable diffusion o Dali puedes crear imágenes hiperrealistas de casas de ensueño y ponerlas en herir bnb a un precio muy jugoso Pues a este tipo de cosas es a lo que se refiere como Deep scams siguiente malware basado en llms esto la verdad me dejó bastante loco resulta que han encontrado hasta tres versiones de malware en github porque lo hicieron como prueba de concepto que se automodificación del malware tiran de la app de Open Ai y se reescriben para que así sea más difícil detectarlos porque están en en constante cambio en constante evolución y por tanto es muy difícil sacar una firma exacta de la muestra del malware comentan que aunque no lo han visto usándose in the Wild No todavía en ataques reales han visto que la prueba de concepto Funciona muy bien esto la verdad bastante loco Luego habla del descubrimiento de Zero days utilizando Inteligencia artificial muchísimos desarrolladores ya a día de hoy usan tecnologías como copilot para analizar su código escribirlo y y bueno buscar problemas para así solucionarlos bien pues los delincuentes también pueden hacer lo mismo pero para explotarlos una vez más no tenemos aquí ejemplos de de que esto esté sucediendo ya es más una premonición pero es muy factible si me preguntáis a mí que mediante Inteligencia artificial un copilot lo que sea tú le pases el código de un proyecto Open source de una librería que utilizan millones de personas en wordpress o lo que sea y y le pidas a la Inteligencia artificial que que te dé los problemas de seguridad que tiene ese código pues y y ahora esto lo escalas para que continuamente esté escaneando todos los cómics a proyectos que son críticos y que te interesa a ti como atacante lo automatizar todo y te llega un email cada vez se ha encontrado un Cross scripting un sql injection un remot cor execution y lo está haciendo la Inteligencia artificial por ti malware automatizado eso es lo último que nos Comenta mico que es de sus temores teme que los ciberdelincuentes empiecen a automatizar las partes de una campaña de malware que todavía hay que hacer manualmente me explico una vez infectada una máquina no con un malware que puede llegarte a través de millones de emails que se mandan Y tú te descargas Pues el documento de Word con macros o lo que sea algún operador criminal tiene que tomar el control y empezar a mandar órdenes al Software malicioso que tienes que acabas de instalar en tu máquina pues para penetrar en las redes de la empresa encontrar información valiosa ex filtrar los datos cifrar contenido etcétera es decir la parte de infectarte está bastante digamos automatizada o o escalable no Porque se envían emails a mansalva y ya está pero una vez está infectado eso avisa al operador y es el que ya manualmente hace lo que tenga que hacer con la cercanía cada vez más evidente a llegar a la Inteligencia artificial general el famoso agi todo

este proceso podría automatizarse la parte ya de Okay ahora que ya estoy dentro de la de la del ordenador pues toda esa parte del command en control no es toma el control la Inteligencia artificial y es la Inteligencia artificial quien envía instrucciones a los implantes que infectan máquinas en empresas gobiernos e infraestructura crítica y ya están preprogramadas para que su prioridad sea robar información cifrar ordenadores borrarlos lo que sea pero que ya no sea un operador que lo tiene que hacer una especio de Terminator virtual ese primer paso a un guerrero no porque programas todas tus inteligencias artificiales para que destrocen los ordenadores o roben la información pero es todavía un Terminator virtual no sé que me pongo aquí poético catastrofista pero es una buena lupa con la que analizarlo y llegados a este punto qué nos queda hemos cubierto lo que se nos viene encima en 2024 nos hemos centrado luego específicamente en la Inteligencia artificial y ahora para terminar la noticia qué hacemos pues yo creo que deberíamos revisitar los incidentes de seguridad ocurridos en 2023 más destacables esto como digamos contraste por un lado y por otro para validar el episodio que hice en enero de 2023 sobre los trends de el año pasado así lo verificamos y tenía sentido No qué os parece a mí me Mola como idea y para añadirlo Pues a nuestra ya tradición de comienzo de año Así que ahora no solo miraremos hacia delante sino también hacia atrás y para ello me quedo con un análisis en este caso de blipping computer sobre lo más destacable de 2023 en cuanto a ataques sufridos por empresas y bueno la población en general son bastantes Así que os cuento solo los más curiosos desde mi punto de vista y cómo no como siempre os dejo las referencias en las notas del episodio destacan Uno de ellos es el 35.000 cuentas de PayPal que fueron hackeadas mediante un ataque de Fuerza bruta con reutilización de contraseñas esto en 2023 lamentable la verdad que PayPal no detectase tanto tráfico hablamos de 35000 cuentas donde se hizo brute forcing de contraseñas y evidentemente son eh utilizando fuentes de listas de usuarios de contraseñas que se publican en internet pues los atacantes lo que hicieron fueron capaces de ir probándolos y conseguir acceso a miles y miles de cuentas de PayPal otro incidente destacable Bueno más que incidente es una investigación porque esta la elegí porque me gusta no solo hablar de lo malo que ocurrió o de los incidentes que ocurrieron en 2023 sino de algo Bastante curioso que es esta investigación sobre exfiltración de las teclas pulsadas en tu teclado mediante el análisis de sonido pues se concluyó que con una demostración de que era posible recuperar el 93 de lo que un Uno estaba tecleando a través de una reunión de zoom O sea me explico que me me me he medio trabado aquí unos investigadores eh son capaces de estar en una reunión en zoom contigo y tú que estás chateando en slack mientras estás en la reunión el sonido que hace tu teclado y que se cuela por el micrófono y va a través de internet al a los investigadores por la llamada de zoom son capaces de discernir El 93 por de lo que has escrito flipa porque estás tú ahí comentando en el chat del trabajo con los compañeros lo pesado que es el proveedor con el que estás hablando y este es capaz de saber lo que estás Te creando Así que ojito con lo que hacéis durante esas interminables reuniones de amigos pero os digo más a lo mejor estás haciendo una demostración compartiendo tu pantalla y te llega lo típico del login page y pones la contraseña y aparte es que el locutor está viendo justo cuando cuando la pones y podría sacar de lo que estás tecleando parte de la contraseña si no toda una locura otro incidente destacable Go deady uno de los hostings más importantes del mundo sufrió un ciberataque y le robaron código fuente pero es que lo curioso de aquí es después de tener malware instalado en sus servidores durante años 1.2 millones de clientes se vieron afectados ya que los atacantes estaban dentro de la red desde 2021 y fijaos que esto de hecho concuerda muy bien con con la predicción de Google de que se van a utilizar botnets durmientes para estar simplemente dentro de la red utilizar Zero days para vulnerabilidades que no sean detectables y poder estar ahí tranquilitos eh con recopilando información pues aquí tenemos un ejemplo

claro bueno otro el ataque por supuesto esto seguro que lo conocéis a la deena hotelera mgm e por supuesto no puede faltar en la lista ataque que pudimos ver sus consecuencias de hecho en directo a través de redes sociales como tiktok e Instagram ya que todos los sistemas estuvieron caídos durante días y la gente no podía hacer checking en los hoteles y se veían todos los vídeos o las máquinas tragaperras que estaban todas fueras de servicio y resulta que las pérdidas se contaban por varios miles de millones a diario una locura y os dejo uno más el hackeo dirigido específicamente contra los empleados de Kaspersky y que denominaron operation triangulation esto lo conocéis porque os lo conté hace apenas unas semanas pero es que es muy destacable en 2023 sobre todo por el uso de varias vulnerabilidades de día cero encadenadas y creo recordar que eran hasta cuatro una locura Y Estas son las cinco que yo destacaría y que reflejan 2023 a ver lo dicho que nos depara 2024 como siempre queridos oyentes muy atentos que reine la desconfianza mantened vuestros equipos actualizados y seguir las buenas prácticas más básicas de seguridad como utilizar contraseñas únicas un gestor de contraseñas y autenticación de doble factor hasta aquí Hemos llegado queridos oyentes Muchas gracias como siempre por quedaros hasta el final recordar que nos podéis apoyar si os gusta lo que hacemos en patreon lo cual hace que esto sea posible os podéis suscribir al podcast nos podéis escribir a podcast @hack pers.com os podéis meter en nuestro canal de discord en tierra.com brdc vamos es que estamos en todos lados y sobre todo en Twitter vamos a seguir creciendo cuentaselo a tus amigos háblales de este podcast de lo guapo que está que seguro que van a aprender algo y además le puedes pasar directamente este episodio porque así ya se van haciendo la idea de lo que ha pasado y y lo que está por pasar Gracias gracias gracias Nos vemos y nos escuchamos en el siguiente episodio Adiós adiós 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 hackers