Boletín *Novedades TIC*

Enero *2020*

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

Enero, 2020

SEGURIDAD INFORMÁTICA

1. UN HACKER DE 18 AÑOS USA EL SIM SWAPPING PARA ROBAR 50 MILLONES DE DÓLARES EN CRIPTOMONEDAS

Fecha: 24/01/2020

Cuando tienes solo 18 años y te consideras un hacker, tienes la tentación de hacerte rico sin pasar por el proceso habitual (formación, trabajo, esfuerzo). Es mucho más rápido hackear a alguien, y robarle el dinero. Pero como ocurre casi siempre, es fácil ser un hacker, pero si te falta la experiencia, te acaban pillando.

Un joven hacker de solo 18 años llamado Samy Bensaci, ha sido detenido en Montreal. Se le acusa de robar 50 millones de dólares en criptomonedas usando la técnica del SIM swapping**.** Es un sistema que exige una cuidadosa planificación, así como robos y estafas a varios niveles. El ciberdelincuente sabía perfectamente lo que hacía.

La técnica del SIM swapping se hizo famosa hace unos meses cuando el mismísimo fundador de Twitter reconoció que le habían robado su cuenta usando este sistema. El SIM swapping consiste en usar una tarjeta SIM duplicada del teléfono de la víctima, para robarle todos sus datos. Si tienes una tarjeta SIM duplicada y conoces la dirección de correo de la víctima, puedes pedir un cambio de contraseña. Gmail te envía un código SMS de verificación al móvil… que recibe el ciberdelincuente, porque tiene una copia de la tarjeta SIM. Google da por buena la identificación, y el hacker puede cambiar la contraseña y hacerse con el control de la cuenta.Como habrás deducido, la clave está en cómo el ladrón obtiene esta tarjeta duplicada. Puede ir a una tienda de telefonía y pedirla, pero para ello necesita algunos datos de la víctima. Las operadoras suelen pedir el DNI u otro dato identificativo para darte una copia de tu tarjeta SIM, si alegas que se te ha roto o la has perdido.

Aquí entra en juego la habilidad del hacker. Puede hacer phishing a la víctima para obtener estos datos, o ser un familiar o amigo que los conozca, o puede intentar engañar al empleado de la tienda para que le haga una copia sin darle los datos que pide, o usar datos falsos. O, como ha ocurrido alguna vez, tener un cómplice que trabaja para una operadora.

No se ha hecho pública la técnica que utilizó el joven Samy Bensaci para hacerse con las tarjetas SIM duplicadas. Lo que si se sabe es que con ellas en su poder (consiguió las de varias personas), accedió a sus cuentas de correo y del banco, y consiguió las claves de los monederos de criptomonedas. En total robó 50 millones de dólares.

Entre las víctimas hay algunas personalidades como Dan Tapscott, el jefe del Instituto de Investigación del Blockchain, y su hijo.Se ha descubierto que todas ellas tenían algo en común: todas asistieron a Consensus, una conferencia sobre criptomonedas que tuvo lugar en Nueva York. Seguramente allí contactó con ellos y obtuvo su dirección de correo, nombres y algún dato más.

Samy Bensaci ha salido bajo fianza de 200.000 dólares hasta que se celebre el juicio, pero tiene prohibido usar dispositivos que tengan Internet, y deberá permanecer bajo custodia de sus padres. Se enfrenta a varios años de cárcel.

Disponible en:
https://www.ticbeat.com/seguridad/hacker-18-anos-sim-swapping-robar-50-millones/

2. CÓMO OCULTAR TU DIRECCIÓN IP DE FORMA TEMPORAL O DEFINITIVA

Fecha: 23/10/2019

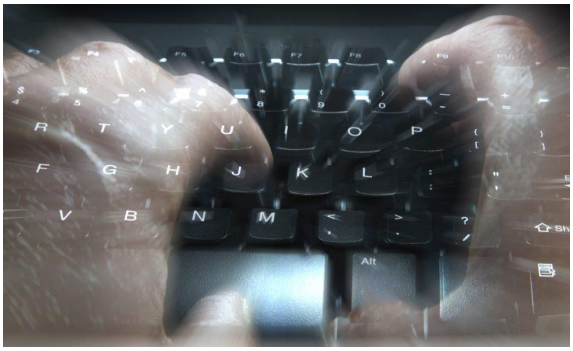
Todo dispositivo conectado a Internet tiene una dirección IP única que lo identifica cuando visita una web o usa un servicio. Es necesaria para mantener el correcto funcionamiento de Internet, pero también sirve para espiarte y rastrear tus movimientos en la Red. Te enseñamos a ocultarla.

Guste o no, es necesario que exista un sistema que permite identificar de forma única cualquier dispositivo conectado online a la hora de realizar actividades tan básicas como enviar un correo, chatear o realizar una compra en Internet. Así nos aseguramos de que el mensaje llegue al destinatario correcto o de que el banco pueda identificar al pagador y al receptor en una compra online, por ejemplo. Para eso se utiliza la dirección IP, una cadena de números únicos para cada dispositivo.

La variante IPv4, la más utilizada, emplea cuatro cifras de 0 a 255. Una dirección IP de este tipo puede ser, por ejemplo, 163.139.12.45.

Existen tantos miles de millones de dispositivos (ordenadores, móviles, tablets, objetos del Internet de las Cosas) conectados a Internet que todas las direcciones IP de cuatro cifras ya se han agotado, por eso ya han comenzado a usarse direcciones IPv6, que tienen ocho grupos de símbolos hexadecimales (números y letras). Algo así como: 2001:0sb9:0000:0042:0000:8d2e:0370:7634.

Cada dispositivo utiliza una dirección IP pública y otra privada. La dirección IP privada es una dirección local que sólo se usa en la red local de la casa, oficina, o donde estés conectado. La dirección IP pública es la del router que ofrece la conexión directa a Internet, y es la misma para todos los dispositivos conectados a ese router. En esta imagen puedes verlo más claro:



Conocer la dirección IP privada es necesario cuando tienes que configurar una red o deseas identificar un dispositivo dentro de tu red WiFi para asignarle unos servicios o bloquear ciertos permisos.

Todos los dispositivos conectados a un router usan la misma dirección IP pública, que es una especie de carné de identidad que identifica tu conexión en Internet. Cada vez que visitas una web, envías un mensaje o usas un servicio, esta dirección queda registrada. Es fácil imaginar el problema: muchas webs, software espía y publicitario usan la dirección IP para espiar tus movimientos o las webs que visitas.

Es fácil descubrir cual es tu dirección IP pública. Basta con visitar alguna de las muchas webs que te la muestran, como por

ejemplo, Miip.es. Esta dirección es única en Internet, y sólo te identifica a tí.

También se usa para bloquear contenidos geográficamente. La dirección IP incluye el pais de procedencia, así que servicios como Netflix la utilizan para bloquear usuarios. Con una dirección IP española puedes usar Netflix España pero no Netflix USA.

Por suerte, existen diferentes métodos para ocultar tu dirección IP. Se utiliza un proxy o una red privada virtual que hacen de intermediario entre tu ordenador e Internet. Tu te conectas a un servidor y ese servidor se conecta a Internet con su propia dirección IP. Todos tus movimientos se registran con esa dirección IP virtual, que no es la tuya real, así que nadie puede identificarte. Además podrás saltarte los bloqueos por zona geográfica.

La opción más sencilla, la web proxy

Si necesitas ocultar tu dirección IP en momentos puntuales porque no quieres que nadie rastree las webs que visitas, lo más rápido y cómodo es usar un webproxy, es decir, una página web alojada en un servidor que hace de intermediario entre tu conexión e Internet. Si ese servidor maneja una dirección IP de Estados Unidos, será como si navegases desde Estados Unidos, así que podrás acceder a servicios exclusivos de ese país. Además también encriptan la conexión para que nadie pueda espiarla.

Existen cientos de webs de proxys gratuitas. Debes entender que al utilizar un intermediario la navegación es más lenta, y suelen incluir bastante publicidad, pero como compartes una dirección IP “de pega” con muchos usuarios, pues realmente estás navegado de forma anónima.

Usar un proxy web es tan sencillo como entrar en la página y escribir la web que quieres visitar en la casilla correspondiente. Por ejemplo, en la web proxy Proxify:

Sólo tienes que escribir la web en la casilla central. Algunos servicios también te permiten elegir la localización del servidor que hace de intermediario, o en otras palabras, el país desde el que quieres navegar.

En ocasiones también es posible configurar el proxy de forma sencilla, por ejemplo elegir si ejecutas o no los scripts de las webs que muestran vídeos, animaciones (que suelen usarse para rastrearte) o si encriptas o no la dirección URL de la web, además del contenido (pues por el nombre de la web se puede saber lo que haces).

Ten en cuenta que un servicio de este tipo oculta lo que hagas dentro de él, pero no otras acciones de Internet, como consultar el correo o chatear por WhatsApp, por ejemplo. Si quieres ocultar la conexión a Internet completa, necesitas una red privada virtual, tal como explicamos en el siguiente punto.

A veces las web proxy gratuitas se caen o van muy lentas, debido al elevado tráfico. Por eso conviene usar diferentes servicios y alternar uno u otro. Echa un vistazo a este enlace.

Protección total con una red privada virtual

Una red privada virtual o VPN funciona de forma similar a una web proxy, pero en lugar de ocultar sólo tu dirección IP en las webs que visitas, oculta todo lo que haces en

Internet, incluyendo envios de mensajes y correos, P2P, etc. Además de esconder tu identidad las redes privadas virtuales encriptan todo el contenido, así que nadie podrá espiar lo que haces. Existen redes privadas virtuales gratuitas y de pago. Las diferencias son fáciles de imaginar. Las gratuitas incluyen publicidad, son más lentas porque mucha gente comparte el túnel de ocultación, y son menos personalizables. Las de pago ofrecen más velocidad y estabilidad, y puedes personalizarlas al máximo. Y no son nada caras. Algunos ejemplos de VPN de pago son ibVPN o G DATA Internet Security Privacy. Existen también abundantes VPN gratuitas, aunque suelen limitar el tráfico diario que puedes usar. Una de las más conocidas es Free VPN.

Tor y su sistema de anonimización

La tercera alternativa que te proponemos es usar Tor, un popular sistema de anonimización que lleva muchos años en funcionamiento. Tor es una red de enrutamiento que oculta tus movimientos al replicarlos por multitud de servidores que forman la red Tor. Tus datos pasan por muchos servidores diferentes antes de salir a Internet, lo que hace casi imposible rastrear su origen. Además toda la información está encriptada. La forma más cómoda de usar Tor es emplear el navegador Tor, que se conecta automáticamente a la red de anonimización y oculta tu dirección IPy los lugares que visitas.

Simplemente descarga Tor desde la web oficial de Tor e instala el software. Ponlo en marcha y usa el buscador incorporado para localizar webs, o escribe su dirección URL directamente.

Disponible en:
https://www.ticbeat.com/lab/como-ocultar-tu-direccion-ip-de-forma-temporal-o-definitiva/

3. ¿PODEMOS CONFIAR EN LAS IDENTIDADES DE LAS REDES?

Fecha: 20/01/2020

¿Quienes somos realmente en internet? ¿Podemos confiar en las identidades e interacciones que existen en la red? Estas son preguntas que a pesar de ser sencillas de plantear, la lógica y mecanismos detrás de ellas son bastante complejos.

Las identidades dadas por plataformas como facebook, twitter o instagram no son en su totalidad seguras y esto tiene consecuencias tan simples como la posibilidad de fingir ser otra persona hasta situaciones que pueden generar conflictos internacionales por la influencia del electorado por medio de divagación de noticias falsas.

Dicho lo anterior, surge la pregunta: ¿Cómo podemos confiar en alguien en la red, siendo un lugar altamente inseguro, pero al mismo tiempo un lugar donde cada vez se centran más nuestras interacciones diarias con otras personas, instituciones, organizaciones o empresas privadas?

Para afrontar esta pregunta, podemos recurrir al termino identidad digital segura y para esto debemos retomar el concepto de identidad física segura. Los responsables de darnos una identidad personal como ciudadanos son nuestros respectivos gobiernos.

Regularmente, se provee de un acta de nacimiento, como primer suceso de vida, en este momento se asignan nombres, apellidos y se nos relaciona con familiares. Posteriormente se dan tarjetas de identidad, de voto, de conducir, pasaportes y en algunos casos identidad militar.

Con este tipo de identificadores, podemos asegurar de manera segura nacional e internacionalmente nuestra identidad para así concluir interacciones como abrir una cuenta de banco, firmar contratos legalmente válidos, adquirir bienes y servicios o viajar de país a país.

Estos métodos de validar nuestra persona son válidos y aceptados por acuerdos nacionales e internacionales. Esto llevado a la era digital ya es posible pero no universal.

Existen países con mayores avances digitales que permiten a sus ciudadanos completas interacciones por medios digitales o regiones con normativas de identidad digital para lograr un acuerdo común entre varios países como el caso de Europa, pero hasta el momento nada mas allá de eso.

La forma de hacer una identidad válida e irrepetible en la red tiene varias vertientes una siendo el gobierno el que genere y corrobore la identidad digital o que la iniciativa privada sea la responsable bajo una normativa estricta descrita por los gobiernos.

La segunda opción da al ciudadano la opción de escoger quién validará su identidad, pudiendo seleccionar a su proveedor de mayor confianza.

Bajo ambos modelos existen también grados de seguridad que aseguran la no duplicidad, falsedad de los identificadores o fácil robo de identidad. A esto, también se le conoce como autenticación de factores.

Dependiendo las regulaciones estos factores pueden ir escalando en complejidad, así que encontramos variaciones que utilizan números pines, huella digital o inclusive reconocimiento facial.

Alrededor del mundo podemos encontrar muchas variantes de identidad digital, tales como la identidad digital de Estonia o su extension e-residency, Aadhaar de la India o el National Digital Identity de Singapur.

El fin ideal de tener una identidad digital como las antes mencionadas es poder conectarse a un ecosistema en el cual los servicios públicos y privados son accesibles de forma remota y aún más importante, que se pueden completar de principio a fin de forma segura en línea.

Finalmente, las características fundamentales para una identidad digital que los gobiernos deben de tomar en cuenta es que; deben de ser únicas y seguras para cada persona, deben estar vinculadas a una firma electrónica (lo que involucra una ley de firma digital), usar al menos dos factores de autenticación, contar con encriptación para proteger la identidad y acciones de las personas y que tengan distribución generalizada, así como usabilidad.

Disponible en:
https://www.tynmagazine.com/podemos-confiar-en-las-identidades-de-las-redes/

BANDA ANCHA

1. 2020 EL AÑO DE LA CONECTIVIDAD INALÁMBRICA

Fecha: 16/01/2020

2019 contempló la introducción de productos con certificación Wi-Fi 6, la implementación de espectro compartido, la disponibilidad de teléfonos y servicios 5G en algunas ciudades y un aumento en el interés por las redes privadas.

Estos nuevos estándares, productos y servicios darán a las empresas más opciones en 2020 en cuanto a cómo satisfacer las demandas más grandes tanto de capacidad y cobertura, así como también cumplir con mayores expectativas del usuario final.

Incremento de Wi-Fi 6 en múltiples sectores del mercado

Comencemos con Wi-Fi 6. Las adquisiciones de puntos de acceso (AP) Wi-Fi 6 aumentarán en múltiples y diversos sectores del mercado, como hospitales, educación y hotelería, para soportar aplicaciones que requieren un gran ancho de banda, incluyendo video 4K, eSports, AR / VR (Realidad Virtual y Realidad Aumentada por sus siglas en inglés), reconocimiento facial y seguridad pública. De hecho, se espera que los puntos de acceso Wi-Fi 6, que ofrecen una capacidad hasta cuatro veces superior al de los puntos de acceso Wi-Fi 5 Wave 2 anteriores, representen la mayoría de APs adquiridos en finales de 2020. Los AP's Wi-Fi 6 implementados en entornos de alta densidad pueden brindar colectivamente la calidad de servicio requerida a un mayor número de clientes con perfiles de uso más diversos debido al empleo de tecnologías como FDMA, MU-MIMO y Target Wake Time.

5G para soportar casos de uso específicos

"La mercadotecnia de 5G en 2019 fue principalmente orientada a los consumidores, pero vemos que los primeros casos de uso real que impulsarán la adopción provienen de implementaciones en edificios. Para habilitar los casos de uso, 2020 verá a los operadores inalámbricos considerando las frecuencias que han adquirido a través de subastas o asignaciones y tomando decisiones tecnológicas para maximizar sus inversiones", mencionó Moises Montaño, Director, Systems Engineering en CommScope CALA.

Esas decisiones tecnológicas afectarán la capacidad de aportar beneficios 5G al entorno del edificio para cumplir con algunos de los casos de uso, incluido IoT, donde las comunicaciones entre dispositivos pueden permitir que miles de millones de dispositivos envíen breves ráfagas de información a otros sistemas, brindando inteligencia a edificios y ciudades con operaciones más eficientes y nuevas capacidades.

Infraestructura para soportar nuevos requisitos

La demanda de ancho de banda suficiente para soportar estas tecnologías y las aplicaciones que habilitarán se convertirá en una prioridad aún mayor en 2020. Vemos

opciones para que la tecnología inalámbrica en el edificio actúe como catalizador en 2020 para el ciclo de actualización de la infraestructura "detrás" de los APs, incluidos los nuevos Switches Multigigabit Ethernet y el cableado de fibra óptica que soportan alimentación a través de Ethernet (PoE).

Los departamentos de TI involucrados en el ciclo de actualización tecnológica durante 2020 implementarán el cableado CAT6A, que admite velocidades de transferencia de hasta 10 Gbps, para evitar cuellos de botella en la red y soportar completamente las nuevas demandas de PoE. Además, para soportar el aumento esperado en la cantidad de datos y de dispositivos, creemos que las empresas gastarán tiempo y dinero en 2020 para evaluar y adquirir Switches Multigigabit Ethernet.

Con la introducción de nuevas tecnologías como Wi-Fi 6, el lanzamiento del uso compartido del espectro, el aumento del interés por las redes privadas y el continuo despliegue de las redes 5G, 2020 será el año en que los consumidores y las empresas serán los grandes ganadores en conectividad inalámbrica.

Espectro compartido para comenzar con casos de uso

El "experimento", como lo llaman algunos, de espectro compartido comenzó en los EE. UU. con la aprobación de la entidad reguladora FCC para comenzar los despliegues comerciales iniciales del Servicio de Radio de Banda Ancha Ciudadana (CBRS). Fuera de los EE. UU., varios países europeos como Holanda, Alemania, Suecia y el Reino Unido también están buscando la manera de otorgar licencias locales utilizando espectro compartido y frecuencias orientadas a celulares. El aprovechamiento del acceso local al espectro en el rango de 3.4 a 3.8 GHz permitirá a las empresas europeas desplegar más fácilmente sus propias redes privadas en 2020. Creemos que 2020 será el campo de pruebas para casos de uso que incluyen IoT industrial y lugares densamente poblados. Uno de los beneficios del espectro compartido incluye la capacidad de proporcionar conectividad para complejos industriales en ubicaciones remotas o temporales, como minería, plantas generadoras de energía, fábricas y bodegas.

Empresas desplegarán redes privadas para tener la propiedad de los datos

Por último, Moises Montaño señala que: "Las opciones adicionales para la conexión inalámbrica en 2020 son las redes privadas, ya sea por medio de redes privadas LTE o por el concepto de "Network Slicing" (el cual permite dividir una infraestructura física común en múltiples redes lógicamente independientes).

El concepto de redes privadas no es nuevo, pero los despliegues CBRS y 5G están haciendo que esta conversación sea un poco más interesante. Las empresas se dan cuenta que, al administrar sus propias redes privadas, retienen la propiedad de datos lucrativos que pueden aprovecharse para fines analíticos y de aprendizaje automático".

A medida que aumentan las implementaciones de IoT, los edificios se volverán rápidamente "más inteligentes". Sin embargo, las implementaciones de IoT y su administración posterior, especialmente dada la naturaleza y las demandas dispares de ciertas aplicaciones, a menudo son todo lo contrario. De hecho, los dispositivos IoT requieren con frecuencia la instalación de redes separadas, lo que implica mayor dificultad para los departamentos de TI y aumenta los costos de instalación y administración.

Disponible en:
https://www.tynmagazine.com/2020-el-ano-de-la-conectividad-inalambrica/

2. QUÉ PAÍSES LIDERAN LA CARRERA POR EL 6G, 10 VECES MÁS RÁPIDO QUE EL 5G

Fecha: 21/01/2020

Con el 5G todavía en una primera fase en la que se está ampliando la cobertura por distintas ciudades y lanzando un número limitado de móviles con esta conectividad, a falta del gran impulso que se espera durante este año, en Asia ya trabajan en el desarrollo del siguiente gran estándar, el 6G.

Este trabajo para lograr 6G se realiza con la perspectiva de que tendrá una velocidad 10 veces más rápida que el 5G. Para lograrlo se están realizando investigaciones en Japón, China, Corea del Sur y Finlandia, pero es Japón el país donde se conoce una mayor inversión en el área.

Desde el Ministerio de Asuntos Internos y Comunicaciones de Japón se ha creado una sociedad de investigación de carácter gubernamental con una inversión de 2.030 millones de dólares para desarrollar el 6G.

Pero, tal como decimos, no se investiga solo en ese país. En Finlandia hay varias universidades e instituciones públicas dedicadas a la labor, en Corea del Sur LG y Samsung han creado grupos de trabajo y en China anunciaron el año pasado que empezaban sus trabajos con el 6G, pero de Japón es desde donde han llegado más datos, presupuesto incluido.

Todo esto no tiene que llevar a pensar que en Japón van mucho más adelantados en cuestión de 5G, según Fossbytes, las compañías también andan en pleno despliegue por el país y todavía es una apuesta para el futuro cercano.

¿Logrará llegar el 6G antes de 2030 y traerá la calculada velocidad 10 veces superior al 5G? Es difícil saberlo, pero al menos queda claro que ya hay quien gasta grandes sumas de dinero en que así sea.

Disponible en:
https://www.ticbeat.com/tecnologias/japon-espera-llegada-6g/

TELEFONÍA MÓVIL

1. EL TIEMPO DE USO DE MÓVIL SUBE EN 2019 HASTA LAS TRES HORAS Y 40 MINUTOS

Fecha: 16/01/2020

De media, cada usuario emplea un 35% más al día en actividades con estos dispositivos respecto a 2017, aumentando también el gasto por consumidor y la descarga de aplicaciones.

Tres horas y 40 minutos al día. Este es el tiempo que las personas pasamos con nuestros dispositivos móviles, de acuerdo al informe The State of Mobile 2020 de App Annie. Esto es un 35% más que el tiempo medio que, según la organización, se empleaba en 2017 en los mercados analizados. Esto, explican, supone un beneficio para las compañías que están poniendo la tecnología móvil en el centro de sus procesos de digitalización.

Por países, Indonesia destaca como en el que más horas se dedican a esta herramienta, más de cuatro horas y media. Sin embargo, no es la que más crece de las principales regiones analizadas: esa distinción le corresponde a China, que ha

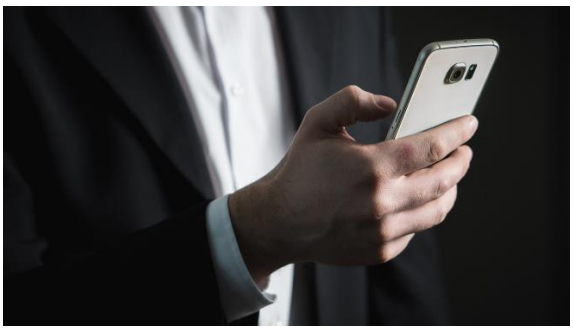
aumentado un 60% respecto al tiempo empleado en 2017.

La duración de la utilización del dispositivo no ha sido el único parámetro relacionado con el uso móvil en crecer. Así, el gasto de los consumidores ha aumentado en un 110% respecto al registrado en 2016 y alcanza los 120.000 billones de dólares en 2019.

Del total del desembolso realizado en aplicaciones, un 72% se corresponde con la categoría de juegos móviles. Las suscripciones de aplicaciones no relacionadas con juegos incrementan su porcentaje del 18% de 2016 al actual 28%.

El país con mayor consumo e incremento es China, que sube un 190% hasta superar los

90.000 millones. Le sigue Estados Unidos, con cerca de 50.000 millones y un 105% más.



En relación a las descargas de aplicaciones, el total anual ha subido un 45% en tres años desde 2016, y un 6% cada año.

En la variable tiempo, el estudio analiza solo datos de móviles Android. Para el consumo económico y aplicaciones se incluye el gasto en tiendas iOS, Google Play y otras aplicaciones de terceros de China.

Disponible en:
https://www.networkworld.es/movilidad/el-tiempo-de-uso-de-movil-sube-en-2019-hasta-las-tres-horas-y-40-minutos

INTELIGENCIA ARTIFICIAL

1. LOS MÓVILES EN EL FUTURO PODRÍAN SUDAR PARA MANTENERSE FRESCOS Y A BAJA TEMPERATURA

Fecha: 23/01/2020

Los científicos crearon láminas de aluminio con un revestimiento a base de metal diseñado para sudar. Al nuevo material lo llamaron MIL-101.

Un grupo de científicos de China dio un paso más cerca de crear un teléfono que sude cuando hace demasiado calor, cosa de enfriarse y así durar mucho más tiempo en operatividad y vida útil.

Muchos mamíferos, incluidos los humanos, transpiran líquido que enfría la superficie de sus cuerpos cuando se evapora.

Los científicos en China que desarrollaron el método innovador dicen que actualmente es demasiado costoso para un uso generalizado, pero es prometedor para una aplicación futura.

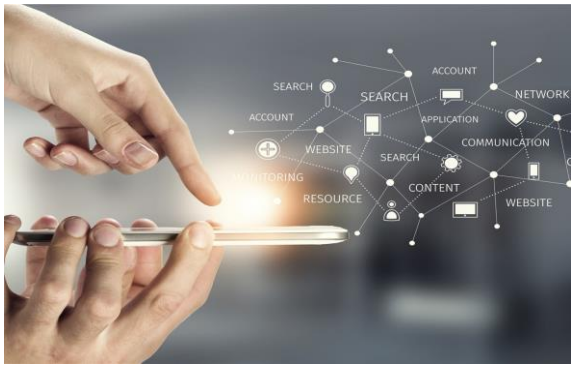
Ellos crearon un recubrimiento a base de metal de solo tres veces el grosor de un cabello humano que mantiene baja la temperatura de funcionamiento de la electrónica al liberar agua.

Cuando esto se convierte en gas y se evapora, lleva consigo el exceso de calor

producido por la electrónica.Podría aplicarse a toda la tecnología, incluidos los dispositivos electrónicos de mano, como tabletas y teléfonos, y ayudar a evitar el sobrecalentamiento.

La gestión térmica

El autor principal, Ruzhu Wang, que estudia ingeniería de refrigeración en la Universidad Jiao Tong de Shanghái, explicó: “El desarrollo de la microelectrónica impone grandes exigencias a las técnicas eficientes de gestión térmica, porque todos los componentes están bien embalados y los chips pueden calentarse mucho”.



“Por ejemplo, sin un sistema de enfriamiento efectivo, nuestros teléfonos podrían sufrir un colapso del sistema y quemarse las manos si los ejecutamos durante mucho tiempo o cargamos una gran aplicación”, agregó Wang.

Los métodos actuales para mantener la electrónica fría incluyen el uso de ventiladores o materiales de cambio de fase (PCM), como ceras y ácidos grasos, que se derriten cuando aumenta el calor, absorbiendo el exceso de energía térmica.

Pero afirman que este enfoque es relativamente ineficiente, y la transición del agua de líquido a gas tiene la capacidad de disipar diez veces esa cantidad de energía.

En un estudio publicado en la revista Joule, los autores publicaron sus resultados que utilizaron menos de 0.3 gramos de material y lograron resultados “significativos”.

Sudar como los mamíferos

Cubrieron tres láminas de aluminio de 16 centímetros cuadrados con un revestimiento a base de metal diseñado para sudar.Llamado MIL-101 (Cr), se aplicó a tres chips, cada uno con diferentes espesores —198, 313 y 516 micrómetros— y los calentó en una placa caliente.

El ancho promedio de un cabello humano es de 75 micrómetros.

Una lámina sin recubrimiento alcanzó los 60 ° C después de 5.2 minutos, mientras que un chip con el recubrimiento más delgado tomó el doble de esta cantidad de tiempo y no alcanzó los 60 ° C hasta que transcurrieron 11.7 minutos.

La lámina con el recubrimiento más grueso alcanzó la marca de 60 ° C después de 19,35 minutos de calentamiento.

“Además del enfriamiento efectivo, MIL-101 (Cr) puede recuperarse rápidamente al absorber la humedad nuevamente una vez que se elimina la fuente de calor, al igual que los mamíferos se rehidratan y están listos para sudar nuevamente”, aseguró Wang.

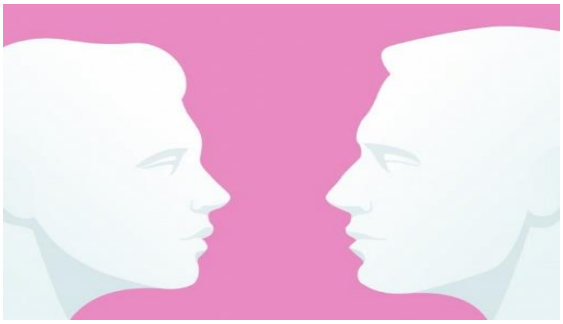
“Por lo tanto, este método es realmente adecuado para dispositivos que no funcionan todo el tiempo, como teléfonos, baterías y estaciones base de telecomunicaciones, que a veces se pueden sobrecargar”, puntualizó.

Para investigar el efecto de enfriamiento de MIL-101 (Cr) en dispositivos reales, los investigadores unieron su material sudado en un chip de computadora.

Disponible en :
https://www.fayerwayer.com/2020/01/moviles-sudar-temperatura/

2. DENTRO DE CUATRO AÑOS 1 300 MILLONES DE MÓVILES TENDRÁN SOFTWARE DE RECONOCIMIENTO FACIAL

Fecha: 10/01/2020



Para 2024, además, se esperan 800 millones de dispositivos con hardware de reconocimiento facial y 4 600 millones con sensores de huella digital.

Las funciones de reconocimiento facial se están abriendo paso en el terreno de los dispositivos móviles, tanto a nivel de hardware como de software.

Según cálculos de Juniper Research, el hardware de reconocimiento facial tipo el Face ID en el iPhone va a ser la modalidad de hardware biométrico que más rápido crecerá entre los *smartphones*. De estar presente en unos 96 millones de terminales acabará sobrepasando la barrera de los 800 millones en el año 2024, de acuerdo con esta consultora.

Sin embargo, el reconocimiento facial basado en software seguirá teniendo más peso. Y es que para dentro de cuatro años se espera que esta capacidad esté presente en más de 1 300 millones de dispositivos, gracias a los avances que se están produciendo en tecnología de inteligencia artificial y su relación con los pagos móviles.

Eso sí, parece que los usuarios preferirán los pagos con huella digital a los pagos a través de reconocimiento facial. No en vano, Juniper Research dice que más de 4 600 millones de *smartphones* integrarán sensores de huella en 2024

Disponible en:
https://www.silicon.es/dentro-de-cuatro-anos-1-300-millones-de-moviles-tendran-software-de-reconocimiento-facial-2410821

3. TENDENCIAS 2020: LA DETECCIÓN COMO FASE ESENCIAL EN CIBERSEGURIDAD

Fecha: 07/01/2020

La inteligencia artificial será la tecnología protagonista en los próximos ejercicios en materia de ciberseguridad. Así coinciden la mayoría de los estudios sobre predicciones tan populares por estas fechas.

No es de extrañar el protagonismo de la IA en los listados. La inteligencia artificial está cambiando y cambiará significativamente la ciberseguridad por diversos motivos; para empezar, porque tal y como recoge una investigación de Ponemon Institute, la inyección de esta tecnología agilizará enormemente los procesos de trabajo como la investigación de vulnerabilidades, el parcheo de redes o la eliminación de falsos positivos.

Los principales expertos en la materia consultados por Forbes anticipan que la inteligencia artificial y el machine learning traerán consigo constantes mejoras en la gestión de bienes de las empresas en general y en la seguridad TI en particular, gracias a la mejora de la resiliencia del endpoint, entre otras cosas. Además, las herramientas continuarán mejorando gracias a diferentes conjuntos de datos lo que darán como resultado una imagen más amplia de las amenazas globales. Los duchos en la materia anticipan un interesante reequilibrio en los presupuestos de los departamentos de seguridad TI: se estima que destinarán más recursos a la detección de amenazas frente a la predicción y respuesta.

Y aquí cabe destacar una tendencia emergente: Threat Hunting. Esta técnica, basada en la búsqueda activa de amenazas que no han activado las alarmas, se perfila como una metodología de futuro por diferentes motivos. En lugar de esperar a que un ataque active una alarma, la búsqueda de amenazas adopta un enfoque integral y holístico para monitorizar e identificar de manera proactiva actividades sospechosas o potencialmente maliciosas con el objetivo de tomar medidas o minimizar, si no evitar, el daño.

Cisco recomienda diferentes herramientas para la búsqueda de amenazas, entre las que se incluyen diversas soluciones inteligentes. Y es que la combinación de métodos tradicionales con tecnologías inteligentes parece ser la fórmula óptima para protegerse ante las amenazas.

Disponible en
https://cso.computerworld.es/cibercrimen/tendencias-2020-la-deteccion-como-fase-esencial-en-ciberseguridad

EMPRESAS

1. HUAWEI ELIGE A TOMTOM COMO SUTITUTO DE MAPS

Fecha: 14/01/2020

El gigante se vio obligado a desarrollar su propio sistema operativo para teléfonos inteligentes, después de que el gobierno de Trump, lo pusiera en una lista negra el año pasado debido a preocupaciones sobre la seguridad nacional.

Estados Unidos prohibió a Huawei usar el sistema operativo Android oficial de Google, junto con aplicaciones ampliamente utilizadas como Google Maps, en teléfonos nuevos.

El acuerdo con TomTom significa que Huawei ahora puede usar los mapas, la información de tráfico y el software de navegación de la compañía holandesa para desarrollar aplicaciones para sus teléfonos inteligentes

El portavoz Remco Meerstra informa a Reuters que el acuerdo ya se había cerrado hace mucho tiempo, pero que el anuncio se hizo deliberadamente: tampoco se revelaron detalles adicionales sobre el acuerdo.

Donde hay voluntad hay un camino

Sin los mapas populares, volvería a faltar un aspecto importante de los teléfonos Huawei, pero ahora es algo limitado. Por el momento, la colaboración con TomTom proporciona la mayoría de la funcionalidad que Maps también ofrece, con al menos una excepción importante: Maps también muestra la ruta más rápida de A a B en transporte público, TomTom no.

Disponible en :
https://www.computerworld.es/tecnologia/huawei-elige-a-tomtom-como-sutituto-de-maps

2. CES 2020 QUÉ ESPERAR PARA LA FERIA DE TECNOLOGÍA MÁS GRANDE DEL MUNDO ESTE AÑO

Fecha: 03/01/2020

Llegó enero y como todos los fans de la tecnología recuerdan, durante los primeros días del año se lleva a cabo la feria más grande de tecnología del mundo, nos referimos a CES en su versión 2020, a la

que nosotros asistiremos y realizaremos una cobertura completa del evento.

Es por esto que, días previos a que se desarrolle el evento, comienza una oleada de rumores y expectativas a través de la web tratando descubriendo que será lo que veremos para la versión que se nos acerca

Recordemos que CES 2020 se realizará entre los días 7 y 10 de enero en el Centro de Convenciones de Las Vegas, ubicado en el Estado de Nevada, Estados Unidos.

CES 2020 y lo que se espera

En esta feria se presentan una infinidad de productos, los cuales marcan sin duda la tendencia que veremos en el año y en los que se avecinan. Durante los últimos años se ha visto una tendencia a la disminución de la tecnología móvil y por el contrario, televisores, computadoras, auriculares, parlantes inteligentes, drones, vehículos autónomos se han visto potenciados en las versiones más recientes.

En total son más de 4.500 empresas de tecnología que exhiben sus productos y servicios en esta feria gigantesca. Es por esto que a continuación trataremos de resumir que es lo que encontraremos y esperamos para la versión de CES 2020.

Televisores: Para esta versión esperamos ver innovación en lo que respecta a la tecnología de las tele, ya que esperamos ver innovación y un acercamiento de las nuevas posibilidades que ofrece la tecnología para potenciar estos productos. Marcas como Apple, Samsung e incluso Google guardan anuncios con respecto a estos dispositivos.

La guerra del Streaming: Durante este 2020 se espera que la batalla por la transmisión de contenidos a través de Internet crezca más, donde plataformas como HBO Max, Disney+, Apple tv y otras más potencien aún más sus servicios. Se espera además que existan anuncios con respecto a diversos acuerdos de licencias de contenidos y la posibilidad que otros gigantes de la industria se unan a esta batalla por el streaming.

PC: Lo que se espera principalmente ver en durante el CES de este año con respecto a laptop es sin duda ver la posibilidad de conocer dispositivos con tecnología plegable, ya que el año pasado algunas compañías pegaron el salto y realizaron muestras de este tipo. La mejora en las tarjetas gráficas y nuevas GPU acompañadas con mejoras en procesadores es algo que también posiblemente veamos durante la versión de la feria este año.

Hardware para juegos: Como ya sabemos, las nuevas consolas de Sony y Microsoft están en camino y las compañías están preparando todo un ecosistema que rodee a estos nuevas versiones de sus principales consolas de juego. Aunque es poco probable que veamos alguna de ellas en CES, lo más seguro es que se veamos un poco más de énfasis en la tecnología 8k, ya que como ambas empresas lo han dicho, sus nuevos juegos vendrán por defecto en esta resolución.

Transporte: Sin duda algo que en CES veremos en mucha cantidad será los autos eléctricos, ya que estos continuarán dominando todas las formas de transporte durante la siguiente década. Aunque todavía queda algo de tiempo con los motores a combustión, este año los

fabricantes en CES esperan presentar productos más "extravagantes", pero no por ellos revelaciones increíbles, ya que la mayoría de estos modelos suelen ser prototipos.

Finalmente, en otras áreas en las que se espera ver más que todo innovación será en los vehículos pequeños eléctricos (scooter y otros), cámaras, tecnología para los hogares inteligentes y en los auriculares, donde se espera que exista un avance considerable en la tecnología de cancelación de ruido.

Disponible en:
https://www.fayerwayer.com/2020/01/ces-2020-expectativas-feria/

MINISTERIO DE COMUNICACIONES

Sistema de Vigilancia Tecnológica