EL LADO OSCURO DE INTERNET

DESCUBRIENDO DATOS Y PRIVACIDAD

TELLY FRIAS JR

El Lado Oscuro de INTERNET: Descubriendo Datos y Privacidad

Telly Frias Jr

Autopublicado por: Telly Frias Jr

Introducción

1. **Internet de las Cosas**
2. **URL Masking**
3. **Llamadas Robot**
4. **Cómo rastrear un clic de enlace**
5. **Internet Impulsado por las ventas**
(programas afiliados e Influencers)
6. **Anonimato en la web**
7. **The Onion Router (TOR) ¿Qué es Tor?**
8 **Red privada virtual (VPN)**
9 . **Caja virtual (V Box)**
10. **Criptomonedas y el Mercado Digital**

-¿Qué es Blockchain?
- ¿Por qué el anonimato de Bitcoin se ve negativamente y por qué no más personas

lo han adoptado como medio de intercambio?

11. **Minería de criptomonedas**
12. **Gana mientras juegas**
13. **Herramientas Online**

-Google Anuncios

-Google Analitica

14. **Vulnerabilidad de Wi-Fi**
15. **Prueba de pluma**

Conclusión

EL LADO OSCURO DE INTERNET

Prólogo

Este artículo presenta a grandes rasgos el tema de "Internet de las Cosas" o Internet of Things (IoT) y su influencia en nuestras vidas. Como continuación de nuestro primer ensayo "Cibercrimen: Las Amenazas al Navegar en Internet y en Las Redes Sociales" discutiremos sobre como nuestros simples electrodomésticos se han convertido en herramientas conectadas a la red en los últimos años y podemos pronosticar que esta tendencia seguirá en aumento. Internet ya cuenta con 3 mil millones de usuarios, es decir, un 43% de la población mundial. Estos usuarios están constantemente conectados a las redes sociales, haciendo compras en linea y participando en otros medios de comunicación. En Estados Unidos el 87% de la población usa Internet. Todos los electrodomésticos electrónicos enchuflables serán conectados a Internet en un futuro próximo. Por tanto, las ciudades gradualmente seguirán siendo más eficaces y convirtiéndose en ciudades inteligentes o smart cities con competencias en sistemas digitales de automatización. En estas nuevas ciudades se podrán prevenir accidentes en las carreteras y automatizar el cobro de las multas a coches teniendo evidencia cámaras de vigilancia. Ésto ya está sucediendo y continuará avanzando la tecnología de comunicaciones.

Internet de las Cosas

A pesar de las regulaciones gubernamentales, laborales y políticas existe un espacio virtual abierto 24 horas al día que nos permite ganar dinero aunque estemos durmiendo una fabulosa siesta. Este gran mercado nos permite ingresos a toda hora y consiste en un medio de conexión y comunicación que está siempre a disposición cuando lo necesitáis. Éste nuevo mundo se llama 'Internet'. Hemos ampliado nuestro conocimiento sobre lo que constituye ser un emprendedor en Internet. Deseo que el lector valore este ciberespacio como una herramienta crítica para su vida cotidiana y sea consciente de lo que está sucediendo en éste mundo cibernético. La hiperactividad en las redes es imposible de manejar por un solo ser humano. Las cuentas de usuarios y sus transacciones son infinitas. Hoy por hoy, los comentarios explícitos sobre la política causan gran polémica en las relaciones publicas o sociales y algunos usuarios aprovechan éstas situaciones inventando nuevos trucos para estafar a otros y se requiere tener mucho cuidado cuando se navega en éste campo virtual.

No es un mundo totalmente anárquico como se presupone cuando se declara que la red oscura o 'dark web' están fuera de reglamentos legales pero como en el mundo real, en Internet existe solo un lado oscuro o redes arcanas que solo es conocido por pocas personas que podrían hacer mucho daño. No obstante la red también funciona entre ellos mismos para poder gestionar sus operaciones clandestinas, y crear un negocio muy lucrativo. Es importante aprender como se hacen las cosas porque cuando enfrentamos a personas sus actos nos podrían decir más que lo diría sus propias palabras. En la primera parte nos centramos en la idea de que la ciberseguridad de un usuario en Internet se convierte en riesgo desde que se hace el primer clic a un enlace. Por consiguiente, dependiendo de los tipos de comando que ofrece un PC u otro dispositivo a menos que no escribas directamente a la computadora, la única forma que normalmente existe para comunicarnos es haciendo un clic con el ratón o un clic con el dedo en tu móvil inteligente. De hecho el iPhone fue el primero en eliminar el teclado en tu móvil. Éste clic se convirtió con pantallas táctiles donde aparece un enlace que te lleva a tu destino. No importa cual sea vuestro objetivo, en todo momento, podríais aplicar éstas mismas técnicas usando las herramientas pertinentes a la solución de un problema de ciberseguridad que te asesora sobre el nivel de confianza o amenaza en éste espacio virtual. Si eres una persona que se recuerda los orígenes del Internet en los años 90s habrás experimentado lo lenta que era una conexión en Internet. El uso de la línea telefónica fue el comienzo. Hace un poco más atrás en los años 70s y 80s antes de computadoras personales el "hacking" era dirigido hacia los teléfonos públicos. En retrospecto, el origen de hacking empezó en las líneas telefónicas.

La red telefónica fue un medio de comunicación desarrollado a medianos del siglo 19 e inventado por el italiano Antonio Meucci. Por otro lado otra innovación de aquella época fue el radio inventado por Gugliemo Marconi. Estos fueron los inicios de la comunicación masiva. La primera Compañía dedicada a proveer servicios telefónicos (al menos en los Estados Unidos) se llamaba Bell Atlantic para luego pasar a ser AT&T y finalmente convertirse en Verizon. En el sector de telecomunicaciones las grandes empresas telefónicas si desean unirse o una corporación adquirir a otros necesitan el consentimiento del gobierno Federal ya que las leyes como el 'Sherman Antitrust Act' de 1890 la primera de las tres leyes "anti-trusts" que en 1914 se hicieron contra los monopolios de las corporaciones y anegarles una abrumadora cuota de mercado. Es más, con las colaboraciones de empresas telefónicas como Sprint/ Nextel y T-Mobile, Verizon y AT&T éstas controlan el mayor porcentaje del mercado. Sin embargo, ellas llegan a acuerdos de cooperación con derechos a las torres antenas de celulares responsables de la difusión de comunicaciones.
Los teléfonos públicos se utilizaban hasta que el gran uso del teléfono móvil los hizo obsoletos desde finales de los 90's fueron vulnerables al hackeado por un pequeño aparato que transmitía un sonido especial. El hacker alzaba el teléfono y con el mismo aparato procedía a pulsar una serie de clics produciendo un sonido de cierta frecuencia auditoria programando la línea telefónica a desviar el pago de la moneda depositada. Asimismo, los hackers de los años 70s y 80s podrían hacer llamadas gratis a cualquier

parte del mundo. La herramienta clave de ésta operación que obviamente fue ilegal se llamaba bluebox. Era por consiguiente ilegal poseer éste dispositivo. Los fundadores de Macintosh, Steve Jobs y Steve Wozniak fueron de los pioneros en usar ésta herramienta. En el primer ensayo hablamos de como ellos lanzaron el i-Phone que ha sido la gran innovación en comunicaciones del siglo veintiuno. Probablemente, hoy por hoy, un smart phone o móvil inteligente es la herramienta más utilizada en nuestras vidas. En gran parte producto de la doctrina 'transhumanista' se pretende transformar la condición humana mediante la aplicación de tecnologías que aumentan nuestras capacidades como seres humanos y hacen que glorifiquemos nuestros móviles inteligentes.

Aparentemente nuestra cultura tecnocrática ha avanzado bastante hoy en día. De hecho, nuestras costumbres y el nivel de confort se han adaptado dependiendo en si se tiene una conexión Internet a través de WiFi. (IoT) Internet of Things es especialmente un tema polémico ya que asisten en nuestras exigencias con la conserje de Alexa, una cafetera que se programa a preparar un café a las siete de la mañana, o un coche se se calienta cuando la temperatura está bajo 0 Grados Cesio. Todos los smart dispositivos contienen con un chip especial que se comunican con la red para hacer actualizaciones de software y hasta funcionar. La desventaja es que estos dispositivos pueden trabajar por el mal cuando no querremos ya que trabajan para seguir sacándonos dinero vendiéndonos más productos.

La impresora es un buen ejemplo, en éste caso digamos que hay una impresora que cuesta entre 90-100 dólares y los cartuchos de tinta cuestan también lo mismo por el paquete completo de blanco/negro y color. Muchas veces las impresoras se venden a una pérdida y el coste se recupera en compras de tinta cada trimestre. La impresora está conectada a la red y ya es un dispositivo producto de 'Internet of Things'. La impresora recibe actualizaciones de software y se mantiene conectado a la red donde gestiona los niveles de tinta y otros aspectos de la impresora. Sabiendo que los cartuchos de tinta contienen un chip especial que mide el nivel de tinta, una táctica que usan las empresas de impresoras es advertirte cuando necesitas más tinta para imprimir. El chip que contiene un cartucho de tinta en una impresora está programado para vivir su vida útil, y además están programados para no ser rellenados y dejar de funcionar si tu no usas los cartuchos de la misma marca de la impresora. Éste servicio alude a la responsabilidad de imprimir a veces dejando de funcionar aunque todavía quede tinta o no. Por otro lado los dispositivos de conserje como Alexa o Siri a veces pueden tener nuestra información bancaria y hacer compras de defecto simplemente porque el dispositivo nos registra en la casa diciendo que nos gustaría tener algún producto o cosa material. Estamos en ésta fase de la tecnología y nuestra capacidad en línea se sigue ampliando con almacenar Big Data.

En éste momento quiero avisaros que no es necesario usar más herramientas físicas de las que vamos a hablar en este artículo- aparte del ordenador para poder hacer una operación en el 'lado oscuro' en la web. A pesar de que se puede hacer mucho con el hardware como servidores, bluebox o keyloggers- que adivinan contraseñas analizando el sonido de botones pulsado en algún teclado y/o teléfono) hay ciertos software que invaden nuestra privacidad. Existen herramientas que almacenan los datos en una red

privada también generadas por empresas que ofrecen servicios de hospedaje en la nube. Tenemos que pensar bien como conducirnos en las redes. De la misma manera debemos saber si queremos prestar nuestros servicios o vender nuestros productos. Si vos sois consumidor y tenéis duda sobre como podéis salir perjudicado participando en las redes sociales ejecutando estos inocentes clics que os lleváis virtualmente a cualquier lugar debes leer éste libro. Aquí aprenderéis a conduciros inteligentemente en Internet y conocerás el uso de algunas herramientas útiles que previenen graves errores.

URL MASKING

La dirección en el mundo cibernético de las redes se denomina Uniform Resource Locator (URL) y ésta no es otra que una dirección electrónica como si fuera una dirección de correos para poder localizaros. Pero en el mundo del cibercrimen existen personas que utilizan el enmascaramiento de ésta dirección localizadora o URL para engañarnos y dirigirnos a distintos sitios webs sin nosotros saber adonde estamos yendo. El propósito de incorporar ésta táctica de enmascaramiento de la dirección web llamado en inglés URL Masking es mostrarnos un enlace con rostro diferente con el objetivo de llevarnos a páginas web desconocidas con archivos corruptos. A pesar de que hay muchas razones por las cuales un usuario incorpora un enlace de éste modo existen dos formas de ejecutar el enmascaramiento. Sabiendo bien que cuando se difunde un enlace en línea todo el contenido está expuesto para las masas. Es un gran riesgo el que tomamos al atravesar un camino en el mundo cibernético cuando no sabemos la dirección de un enlace y hacemos un clic en buena fe. El nivel de vulnerabilidad cuando se trata de encontrar un enlace enmascarado se mide entre un rango de riesgo de 0-100% porque depende de si nuestros sistemas toman las medidas (a veces necesarias) de evaluar el nivel de amenaza ya que un enlace enmascarado no tiene dirección propia (web oculto) y podemos ser engañados si no tenemos cuidado. Se trata de cuantificar variables como: antivirus- ¿Tenemos un antivirus? la audiencia, los seguidores y los temas interesantes al cual nosotros frecuentemente escribimos. Cada vez hay más gente propensa a captar la información periodística, vídeos y publicaciones escolásticas por medios digitales. En un **Informe Anual de la Profesión Periodística** "el 75% de los españoles citaba la televisión en primer lugar, mientras que al 48% las noticias les llegaban a través de las redes sociales." Sin embargo, la división cultural por parte del auge tecnológico y la forma tradicional es bastante polémica ya que la forma digital no ha eliminado completamente el uso del papel. A pesar de iniciativas verdes fundadas por las ONGs ecologistas que persiguen el desuso de papel y el hecho de que se fomentan cada vez más intercambios y transacciones digitales pero la forma tradicional no ha sido superada todavía. Un ejemplo de "enlace enmascarado de la dirección web" puede ser un enlace para hacer compras o enviar dinero. Un enlace enmascarado puede llevarnos a cualquier parte de la web y, a menudo, los influenciadores o el contenido popular nos guían para hacer clic en estos enlaces. Constantemente aplicamos el reto de capacitarnos y adquirir mejor información para atraer un audiencia a nuestra red. La información que suele pasar a las masas de

usuarios se conoce como el "efecto viral". Gente influyente en las redes sociales usa la práctica de hiperenlaces para vender algunos productos ofreciendo códigos de descuento como incentivos. De hecho, hay demasiado contenido en las redes sociales, que incluye los hiperenlaces que manipulan enmascarándose como otras direcciones web. No obstante, hay que reconocer que nosotros estamos siendo dirigidos por los miles de millones de usuarios en Internet. En éste capítulo describiremos como usar el enmascaramiento de las direcciones web en una página virtual. Y además presentaremos algunas herramientas de la web que nos podrían ayudar llevar a cabo nuestro objetivo de enmascarar un enlace. Por siguiente, identificaremos cuales son algunos motivos del enmascaramiento de la dirección web y por último miraremos soluciones como protegernos al enfrentar un hiperenlace o "hyperlink" de ésta categoría.

Realmente, adquirir un nombre de un dominio en las redes o web domain names no es totalmente gratis. De hecho, no podemos tener una página web sin pagar por los derechos al servidor a menos de que tengamos un sistema de servidores y una compleja red de dispositivos. Después de obtener el nombre de un dominio reservamos el nombre de este dominio (esto incluye los .com, .net .es, .pt, .de) de forma similar como obtenemos las direcciones de nuestras casas. Para instalar una página web se puede gastar entre 20 y 100 dólares en el desarrollo y mantenimiento de una página web quizás más o menos en el primer año. Personalmente hemos experimentado con Wix, GoDaddy y WordPress y otros posibles hosts de dominio para la gestión y administración requerida en activar una simple página web. Para cumplir con este objetivo se requiere conocimiento de la aplicación de HTML que mostramos aquí. Por ejemplo texto del enlace existen dos partes distintas en el guion <a href="˝"> y este mismo se puede interpretar como lo que está escrito entre comillas es la dirección de la pagina web "**www.camisasyropabarata.es"** Por consiguiente, la otra parte clave es mirar hacia el texto, lo que está escrito entre los paréntesis angulares. En éste caso, el texto subrayado en azul se percibe como la dirección de la pagina web. Aquí el texto o el rostro del hiperenlace está escrito como "haga clic al enlace" Haga Clic al Enlace En ésta parte estas letras se instalan como la fachada del enlace o bien el rostro de la fuente. En pocas palabras, el texto azul es el hiperenlace que se verá ante el publico. Ya que hemos visto un poco de HTML acerca de enmascaramiento de nuestro correo electrónico ahora bien vamos a ver la segunda manera de hacer éste enmascaramiento. Antes que nada en éste capítulo también discutiremos sobre cuales son las posibles motivos de enmascarar un correo electrónico como esta práctica afecta usuarios a partir de las redes sociales. En el ensayo anterior explicamos formas en que podríamos ser vulnerables a estafas y ciertas amenazas en la web como los ataques de robo de identidad que ocurre a través de tipos de enlaces enmascarados en éstas mismas plataformas. Concluimos que los ataques de suplantación de identidad conocido con el termino phishing en ingles y estas son nada menos que amenazas retratadas en forma de enlaces siendo un componente de alto riesgo; la realidad es que los ataques de robo de identidad se encuentran fácilmente por los correos electrónicos, las redes sociales y algunas otras páginas web.

Desafortunadamente, para crear una página web hay que pagar por los derechos al servidor anualmente. Algunos países como España requiere identificación para ser propietario de un sitio web con el dominio ".es" porque el

gobierno lo impone ante la ley que lo interpreta como una fuente de ingresos y para ellos mismos cobrar impuestos. Sin embargo ahora mismo hay disponibilidad de los sitios web, a saber, dominios como .com, .net etc que están a la venta. Un pequeño emprendedor puede tener una página web (no publicada) gratuitamente en la web en condición de si se mantuviera parte de un host con exigencia de darse en alta. Por ejemplo, tenemos una dirección que deseamos llamarlo "camisas y ropa barata". Usando la plataforma de Wix.com nuestra dirección (si no ha sido reservada) podría ser www.wix.com/camisasyropabarata. Unos de los motivos por los cuales se usa la herramienta de enmascaramiento de la dirección web es para simplificar el texto del enlace que de igual manera al hacer clic nos llevará donde querrá. Por lo visto usar la herramienta tiny.url simplifica el enlace que podría resultar en tinyurl.com/tt4yhfYt. Probablemente te preguntarías sobre cual es el motivo al cortar el enlace más o menos nueve o diez palabras. La respuesta es que la simplificación es parte del éxito de negocios. Considere que muchos de los conglomerados que existen hoy en día en el mercado se sostienen con un solo nombre y en cuanto más corto el nombre mejor porque será fácil para la gente recordarlo. En Estados Unidos Walmart es el líder en venta al por mayor en la industria de retail. El nombre Walmart contiene dos silabas. Al nivel mundial existen Amazon, AliBaba y eBay empresas que se han engrandecidos por Internet. De igual manera, sus nombres son fácil de recordar ya que sus nomenclaturas no abarcan mucha letras.

Asimismo los motivos de montar una técnica de enmascaramiento de nuestro dirección web podría ser buena para negocios ya que un enlace nos lleva a destinos mercantiles en función de comercios electrónicos. Realmente, el mundo de Internet de la misma forma que el mundo real esta inundado de vendedores. Es decir, en las redes sociales, en grupos de chat y en páginas web todos ellos sirven como un medio publicitario para vender productos o servicios. De hecho, cualquier intercambio tiene por un lado un producto o servicio para vender. Un vendedor podría ser el anunciante, un amigo en las redes sociales hasta los mismos buscadores cobran sus honorarios por llevar el usuario a la caja de la venta. Todo funciona así, un vendedor en línea puede ser emprendedor vendiendo sus propios productos y/o también trabajando en una cuenta de afiliados donde los vendedores podrían ganar sus comisiones en el acontecimiento de vender productos para una empresa. Hay muchas empresas que se inscriben en estos programas como estrategia de marketing para aumentar las ventas en el sector del comercio electrónico. Un vendedor en línea adscrito a una cuenta de afiliados si ejecuta una venta puede ganar entre el 1 y 10% de la venta total. Pues entonces me preguntarás como conseguir este tipo de ingreso pasivo? A continuación, hay una gran cantidad de plataformas con sus puertas abiertas para reclutar vendedores terceros o vendedores third-party. Rakuten es una plataforma que se une a la red con una multitud de comerciantes en línea para vender prácticamente cualquier tipo de producto. La ventas de libros, electrónicos, electrodomésticos etc. incluye el almacenamiento de datos en la nube. Otro ejemplo es Amazon. La potencia mundial conocida hoy como 'La Tienda de Todo" o "The Everything Store" también cuenta con su programa de afiliados entre muchos otros como un sistema de lucro para llegar a mas compradores. Amazon mismo empezó como un tienda de libros. Entre Rakuten y Amazon hay cierta competencia porque sabemos ya que ambas plataformas venden de todo en términos de tipos de productos también hay que mirar a los otros sectores correspondientes donde ellos mismos suelen competir en mayor grado como en la nube y la almacenamiento de Big Data. Amazon web services, Microsoft Azure, Facebook, Google son entre las más grandes empresas de Internet con grandes servidores que han tenido mucho éxito vendiendo espacio de memoria en las nubes.

En una encuesta reciente realizada por McAfee, se reveló que el 97% de los consumidores no podían identificar correos electrónicos de phishing. Esto es un problema donde referimos al medir el nivel de amenaza de un enlace. Por cierto hay muchos ataques que pueden venir hoy en día por correo electrónico o por las redes sociales que contienen un enlace sospechoso. Para empezar hay que evitar abrir una carta con una dirección web extraña. Parte de la ecuación

también se propone en las redes sociales allí mismo donde podríamos encontrar enlaces publicados en los registros públicos de Facebook, Twitter, YouTube y en la sección de comentarios de fuentes periodísticas populares. Los ataques de robo de identidad incluyen enlaces que graban información bancaria como un nombre de cuenta y contraseña. Como solución para determinar si un enlace es producto "puro" tenemos mejor que acudir al ratón y llevarlo a descansar encima del texto azul subrayado. Al descansar nuestro ratón por encima de dicho enlace, nuestro explorador de Internet nos indica por debajo en la parte izquierda de la pantalla donde cita la dirección del enlace y nos avisa sobre éste mismo enlace al hacer clic a donde nos pretende llevar. Aunque de frente probablemente el enlace no diga la dirección web, el texto indicado por debajo en la parte izquierda del explorador de Internet es una solución que nos releva el destino de un enlace.

En el capítulo como rastrear un enlace veremos como rastrear una ubicación a través de la clic de un enlace. Obviamente la solución de disminuir los riesgos hacia la ciberseguridad es teniendo una protección de antivirus. Un antivirus prohíbe la conexión de un enlace malicioso con el ordenador y además advierte al usuario antes de establecer una conexión y acceder al sitio web. También hay páginas webs que sirven como herramientas en línea y pueden escanear bien el enlace hasta clasificar el nivel de amenaza. Todo lo que tienes que hacer es realizar una búsqueda. Para ejercer éste tipo de investigación, software como Norton Safeweb un elemento de protección antivirus que prepara el análisis de ciberseguridad con respeto al enlace. Después de escanear el enlace con nuestra herramienta obtenemos un resumen del diagnóstico y dado los resultados determinamos si el enlace presenta riesgos o no. Para comprobar la validez de un enlace y acertarse de si el enlace es seguro hay que visitar algunas fuentes dedicadas en proveer éste servicio gratuito de ciberseguridad. Remitimos las siguientes páginas web como asesoramiento sobre enlaces dudosos y/o hiperenlaces: http://checkshorturl.com/, http://URLvoid.com, https://ScanURL.com Cada uno de estos sitios web analiza el nivel de riesgo asociado con un enlace. En URL void.com por ejemplo el resumen puede incluir toda la información del enlace como la ubicación, dirección IP de la página web, y la fecha de inscripción del dominio. Por lo visto también contamos con un diagnostico fuerte que está compuesto por un esfuerzo colectivo de peritos en la rama de ciberseguridad. De hecho, el resumen incluye los resultados de más de 38 proveedores de ciberseguridad que examinan el enlace identificando si hay vínculos a malware, robo de identidad, estafas monetarias y estafas de Bitcoin, y Google y hasta un compromiso de nuestra ubicación.

Llamadas de Robot

Hay muchas estafas en los Estados Unidos hasta la fecha. La única estafa en particular que me gustaría discutir muy brevemente en esta sección incluye llamadas automáticas. Un día puede recibir una llamada automática con un mensaje genérico o advertencia. Las llamadas automáticas consisten en un software de voz que es texto a voz y leerá en voz alta una secuencia de textos y símbolos. Las llamadas automáticas pueden programarse para marcar diferentes números de teléfono consecutivamente y configurarse para reproducir la grabación tan pronto como conteste el teléfono. De esta forma, se cree que la operación se hace más eficiente que los humanos porque las máquinas funcionan constantemente. Estas llamadas automáticas también se utilizan para disfrazar la identidad de las personas involucradas que pueden no poseer un nivel estándar de habilidades de habla inglesa y, sin embargo, afirman estar trabajando para el Gobierno Federal. A pesar de su reclamo, el estafador que probablemente obtuvo su información de contacto en línea cuando lo ingresó para un concurso / obsequio o en otro sitio web buscará dinero de usted dándole un ultimátum. "¡O paguen o los arrestaremos!" Incomprensiblemente, estas amenazas pueden derivarse de funcionarios gubernamentales falsos que pueden afirmar que hay una orden de arresto a menos que pague una cantidad específica de dinero.

Hay varias cosas que puede hacer para poner fin a las llamadas automáticas. En primer lugar, debe evitar ingresar su información de contacto como correo electrónico, dirección y, especialmente, número de teléfono en sitios web cuestionables. Hay una nueva ley de llamadas automáticas que debería proteger a los consumidores. La ley TRACED, que es una ley que fue firmada por el Presidente Donald Trump, facilita a los consumidores detectar las llamadas automáticas y evitar responderlas. En efecto, esta ley requiere que las compañías de telecomunicaciones implementen un sistema auténtico de números de teléfono gratuitos para ayudar a los usuarios a identificar las llamadas automáticas. Además, hacerse pasar por funcionarios del gobierno es un delito y, según esta ley, se incrementan las sanciones para estos impostores. A lo largo de los años, este fenómeno de llamadas automáticas y las molestias del telemercadeo han creado desconfianza entre los clientes, ya que más del 70% de los consumidores afirman que no contestarán el teléfono a menos que sepan quién los está llamando y otro 62% dice que

la mayoría de las llamadas van directamente al correo de voz de todas formas. En consecuencia, no puede denunciar a un estafador directamente al Gobierno Federal, incluso si son impostores, a menos que haya sido víctima. Sin embargo, hay fuentes que lo ayudarán a neutralizar estas amenazas. Stopcallingme.ca es un sitio web que le permite informar sobre llamadas fraudulentas y llamadas automáticas. Una vez que cargue el número de teléfono del estafador en el sitio, realizarán una rigurosa verificación de antecedentes para verificar si el número de teléfono pertenece realmente a un estafador. Todos los números de teléfono legítimos no serán seleccionados. Lo que hace este servicio es que una vez que se ha determinado que el número de teléfono pertenece a un estafador, comenzarán a bombardear el número de teléfono con una cantidad exhaustiva de llamadas generadas desde diferentes números de teléfono hasta el punto en que la línea quede inutilizable. También hay un montón de dispositivos y aplicaciones que pueden bloquear automáticamente las llamadas automáticas y los vendedores telefónicos a través de filtros y evitar que se comuniquen con usted. Como siempre, tenga cuidado al ingresar su número de teléfono en línea. En el próximo capítulo, hablaremos sobre cómo se puede rastrear a alguien simplemente haciendo clic en un enlace.

Estafas

En Europa, el monto del fraude en 2012 se calculó en 144,3 millones de euros, según Euro monitor International, y en 2016 estas cifras ascendieron a 1,800 millones de euros. Como puede ver, la escena clandestina de cibermatón está siendo impulsada por la desgracia de los ciudadanos trabajadores. No tiene que preocuparse por ser asaltado en la calle, ya que aparentemente también puede ser asaltado en el ciberespacio, todo debido a un paso en falso que tomó mientras navegaba por la web. En el comercio del mercado negro, estos delincuentes pueden vender cursos, drogas, información de tarjetas de crédito y maquinaria con un servicio de mensajería para entregarle los productos. En Portugal, la policía arrestó a seis piratas informáticos: cinco hombres y una mujer responsables de llevar a cabo una operación de "descremado". El sindicato usó "skimmers", un dispositivo de deslizamiento de tarjeta electrónica que no es como los utilizados por los cajeros, sino más bien aquellos utilizados para iniciar sesión u obtener acceso a un área restringida de un edificio. Aunque, el objetivo principal de este dispositivo es copiar la información de pago. El dispositivo copia la información de pago

pero no le carga dinero a la tarjeta. Esta herramienta es simplemente una forma de copiar información de la tarjeta y transferir los números a otra tarjeta en la que imprimen en la misma instalación. El cardado es una técnica utilizada por los delincuentes del mercado negro y, en retrospectiva, se representa en la película Hackers (2016). La Unidad de Delitos Cibernéticos y del Crimen Tecnológico (UNC3T) estimó que estos seis piratas informáticos entre las edades de 21 a 51 años en Portugal causaron daños por alrededor de 275,000 euros. Alemania ocupa el tercer lugar a nivel mundial en términos de ataques de phishing (justo detrás de los EE. UU. Y el Reino Unido), con USD 386 millones de pérdidas. En toda Europa, verá casos de estafas como en cualquier otra parte del mundo. Según FICO, el fraude con tarjetas aumentó en Italia hasta alcanzar 56,8 millones de euros en 2013. El fraude falsificado representa la mitad de este total (28,4 millones de euros) y se atribuye en gran medida al uso dentro del Área Schengen. A nivel nacional, las transacciones con tarjeta no presente ahora representan el 25% del fraude (EUR 14,2 millones) y las tarjetas perdidas y robadas el 18% (EUR 10.2 millones). En 2015, la Guardia di Finanza, Europol y el FBI realizaron una operación de tormenta con 130 miembros para irrumpir en 32 lugares para arrestar a un grupo de estafadores, principalmente ciudadanos nigerianos, responsables de una operación de fraude romántico que supuestamente intentaban obtener boletos de avión. De sus posibles víctimas Las autoridades lograron recuperar 2.500 millones de euros.

Cómo rastrear un clic de enlace

Podemos incrustar una función de seguimiento en nuestros enlaces de URL (localizador de recursos universal) para rastrear la ubicación de una computadora o usuario de dispositivo inteligente visitando ciertos sitios web que generarán estos resultados deseados. Todo el proceso generado contará y registrará la cantidad de veces que se hizo clic en un enlace, así como detectará la fuente o la ubicación geográfica de cada clic del enlace. Se realizará un análisis o diagnóstico del clic en el enlace. Realizaremos una prueba para rastrear nuestro objetivo entre la demografía existente. Todo esto nos proporcionará la evidencia adecuada para el caso y el punto de determinar si nuestra contraparte está revelando la verdad sobre su ubicación y / o está tratando de estafarnos. Las estafas telefónicas más comunes en los Estados Unidos son la estafa de préstamos estudiantiles federales y la (s) estafa (s) TAX / IRS y las estafas de soporte técnico de Microsoft realizadas por operadores telefónicos indios en alta mar, así como algunos otros. A continuación encontrará las 10 estafas más comunes que se realizan a través de plataformas de teléfono, correo electrónico y mensajería instantánea.

Las 10 estafas más comunes: fraude romántico, soporte técnico, recaudación de impuestos, estafa de herencia, estafa de inversión empresarial, estafa de boletos de avión y visa, estafa de personal policial y militar falso, estafa (s) de trabajo y listados clasificados, estafa (s) de donaciones de caridad .

Problema: Cientos de millones de dólares en riesgo cada año.

Ingresos esperados diarios: EUR 150,000

Ingresos esperados anuales: EUR 100,000,000

Resolución: 70 personas arrestadas acusadas de extorsión, suplantación y delitos de tecnología de la información.

Una víctima informó haber pagado EUR 60,000 solo para evitar cargos de evasión de impuestos y otra más de EUR 7,000 en una sola transacción para resolver disputas del IRS. Estas estafas provenientes de la India a menudo involucran a operadores telefónicos que participan en telemercadeo masivo dirigido a estadounidenses mayores de 18 años. Las víctimas de mediana edad y mayores a menudo gastan más dinero que los estudiantes universitarios recién graduados. Si bien muchas de las estafas telefónicas provienen de operadores telefónicos indios, el público también es blanco de estafadores en línea donde los ciberataques de Nigeria y Ghana usan imágenes de modelos atractivos para atraer a las víctimas desprevenidas y atraerles dinero. Una víctima pagó EUR 300.000 dólares por fraude romántico. Sin embargo, se dice que se sabe que los estafadores por correo electrónico obligan a sus víctimas incluso por todas las cantidades de dinero, como, por lo menos, entre EUR 500 y EUR 3.000 a EUR 5.000 en una sola transacción para liquidar multas con el gobierno o pagar el falso soporte técnico de Microsoft Windows y la resolución de virus de ransomware, así como las estafas íntimas relacionadas con engañar a las personas para que paguen el procesamiento de la visa y el viaje en avión. Muchos estafadores a menudo afirman que necesitan dinero para liberar fondos de una herencia de un millón de dólares o una cuenta bancaria congelada. Además, 63 sospechosos fueron arrestados en 2019 por la policía de Nueva Delhi que operaba estafas de soporte técnico, haciéndose pasar por personal de soporte técnico en Microsoft, Google, Apple y otras compañías tecnológicas importantes. Se investigó que han estado trabajando durante los últimos dos meses en más de 26 centros de llamadas. Lo triste es que muchos de los estafadores no tienen remordimiento por sus acciones y la avalancha de ataques ha puesto en riesgo la información de las personas junto con cientos de millones de dólares cada año para norteamericanos, estadounidenses y canadienses por igual. En conjunto, las 10 estafas más comunes que ocurren en este momento a través de llamadas telefónicas y estafas por correo electrónico comprenden una gran parte de la industria del mercado negro en el mundo de la tecnología. Muchos de estos tipos de estafas implican la solicitud de dinero a través de tarjetas de Google Play o tarjetas de regalo de iTunes para convertirlas en criptomonedas o transferencias de dinero para cobrar en una Western Union local. Sin embargo, la cantidad de estafas (generalizadas y desenfrenadas en América del Norte) se derivan de haber visitado un sitio específico (ya que las cookies nos pueden rastrear) o por correo electrónico de 1 a 1

y comunicación de mensajería instantánea. En muchos sentidos, nuestra información en línea podría verse comprometida. Por ejemplo, supongamos que acabamos de conocer a una persona en línea a quien creíamos que era confiable. Pueden acercarse a nosotros, prometiendo a menudo darnos un lucrativo retorno de la inversión o eliminar nuestra deuda financiera personal. Él / ella puede afirmar que es un multimillonario (s) e incluso retratar ciertas características que admiramos. En cualquier caso, eventualmente desarrollaremos razones para sospechar que alguien es deshonesto, especialmente personas a quienes nunca hemos conocido antes de pedirnos dinero en una plataforma virtual. Dada esta especulación, para aclarar mejor cualquier duda o inquietud sobre la ubicación del objetivo, debemos emplear la táctica de rastrear los clics en los enlaces para revelar IP, nombres de servidores host y ciudad y estado.

En este artículo demostraremos cómo rastrear un enlace utilizando una plataforma de recursos de sitio web automática recomendada. Podemos estar en una situación en la que nos haya contactado un estafador telefónico o un estafador por correo electrónico. Para reiterar, se nos puede contactar con respecto a la deuda pública o la recaudación de impuestos y / o la deuda de préstamos estudiantiles, etc. En cualquier caso, nuestra especulación es la causa de la siguiente acción de investigación. Por lo tanto, suponemos realizar un viaje en la prueba para ver si un usuario en comunicación con nosotros es confiable y transparente. Recuerde que es importante guardar el enlace que usará con la función de código de seguimiento incorporado habilitada, ya que nos permitirá hacer referencia a los resultados de la investigación de seguridad cibernética pertinente.

Presumiblemente, proporcionaremos algunos enlaces de recursos para usar que rastrearán la ubicación de un clic en el enlace. Asegúrese de utilizar esta herramienta con fines éticos. En un ejemplo, supongamos que hemos recibido un correo electrónico de un presunto estafador. El correo electrónico puede solicitarle que ingrese información confidencial, como su nombre de usuario, contraseña o permitir el acceso a su lista de contactos u otros datos. Aquí podemos ejecutar nuestra prueba para detectar fraudes. Si nuestro estafador telefónico o estafador por correo electrónico nos está contactando con respecto a una deuda tributaria, la llamada o la dirección IP de la persona deben proceder de una dirección nacional del estado de EE. UU. En primer lugar, tendríamos que copiar y pegar un enlace en la barra de búsqueda de grabify.link, generar código de seguimiento, copiar y pegar el nuevo enlace en un correo electrónico o chat de mensajería instantánea para enviarlo de vuelta al estafador. Debe guardar el enlace y conservar la página web que generó el nuevo enlace para monitorear los resultados de los datos. La parte difícil aquí es asegurarse de que el estafador haga clic en el enlace para poder rastrear su ubicación. Cuando el objetivo haga clic en el enlace, podremos ver dónde están. Muchas de las causas de nuestras sospechas se basan en los tipos de estafa diseñados para robar dinero de personas como las estafas de romance a través de Facebook, donde se crean perfiles falsos para atraer a las víctimas. Si, por ejemplo, estamos chateando con otro usuario que dice estar en algún lugar de Pensilvania mientras su ubicación precisa (se revela a través del código de seguimiento del enlace generado a través de grabify.link) para estar en algún lugar de Ghana, entonces sabemos que nuestro sospechoso es culpable.

Muchos de estos tipos de factores de prueba antimonopolio pueden reforzar nuestra adhesión para implementar y aplicar medidas de ciberseguridad en nuestra experiencia digital. Pero espera ... ¿Qué pasa si nuestro objetivo está usando una VPN? ¿Una VPN no disuade la visibilidad de nuestra dirección IP? Si bien es posible que podamos cambiar la ubicación detectada de nuestro dispositivo inteligente, PC o computadora portátil, hay formas de determinar si alguien está usando una VPN porque nuestro código de seguimiento identificará si el enlace de enlace está alojado en servicios especiales basados en la nube. Esta es una táctica generalizada utilizada por muchos usuarios de Internet. En última instancia, la identificación de la ubicación de esta manera es utilizada igualmente por los expertos en espionaje y / o contraespionaje. Recordemos en el libro Cybersecurity: On Threats Surfing the Internet and Social Media discutimos la entrevista con el presidente Vladimir Putin y Megyn Kelly donde respondió a las acusaciones de intromisión en las elecciones presidenciales de EE. UU. Y atestiguó cómo a pesar de la ubicación de las direcciones IP y específicas Scripts toda la evidencia apunta a Rusia, estas fuentes podrían ser fácilmente manipuladas mediante el uso de una VPN. De hecho, esto es cierto porque si un usuario está en línea y en cualquier situación dada puede conectar a un usuario a un nuevo host virtual y proporcionar una conexión segura con datos cifrados. Por ejemplo, para un usuario de Internet en Seattle, Washington, él / ella puede configurar la ubicación de la VPN en la ciudad de Nueva York, o prácticamente en cualquier otro país del mundo, como ciudades en países de América del Sur, Europa, África, Asia e incluso partes del Medio Oriente.

Una forma de identificar si nuestro objetivo realmente está usando una VPN, sería habilitar la función de "registrador inteligente" que se proporciona en el sitio web grabify.link antes de generar el código de seguimiento. Aquí veremos si el usuario está usando una VPN. Mediante el uso de esta herramienta, cualquier persona también puede consultar a su ISP- Proveedor de servicios de Internet, cuando en situaciones en las que no tenga una red privada y segura, es posible que su ISP (como: Comcast, Verizon, Spectrum, Time Warner, etc. o cualquier otra compañía de telecomunicaciones por Internet) estarán expuestos. Si un usuario tiene una VPN, aparecerá el nombre de host dándonos el sitio web del servidor host. La forma en que estos enlaces se transmiten a través de la apertura de cookies y ventanas es cuántas víctimas son rastreadas, atacadas y engañadas. Desafortunadamente para la mayoría del acceso a los sitios web, las cookies deben estar habilitadas para que podamos continuar en línea. Si no habilitamos las cookies en nuestro navegador, a veces nos vemos obligados a salir del sitio. En otro capítulo aprenderemos más sobre Google Analytics y cómo se usa para encontrar a los usuarios activos en un sitio web específico. Podremos ver información más completa en ese capítulo junto con imágenes y diagramas de cómo funcionará para nosotros.

Internet impulsado por las ventas

Programa de Afiliados e Influencers

Affiliate Marketing es un programa de recompensas basado en ventas en línea facilitado a través de enlaces (URL) y pancartas. Si no has oído hablar del marketing de afiliación antes de seguir leyendo, aprenderás los conceptos básicos al final de este capítulo. Dado el auge de las redes sociales en la forma en que las personas están conectadas, es viable tener una estrategia de ventas digital óptima para generar ingresos pasivos. Después de todo, ¿no sería maravilloso que me paguen por hacer poco o nada de trabajo? Si alguna vez has visto un vídeo de YouTube en un producto promocional, una publicación de Facebook o una publicación de Twitter que recomienda un producto, es probable que hayas encontrado un enlace de afiliado. Dada la segmentación de los grupos y canales sociales, el dinero, el poder y los intereses se dispersan. En primer lugar, ¿qué es un enlace de afiliado? Un enlace afiliado es una URL única a un producto o servicio específico asignado a un miembro afiliado. Si bien cada producto puede contener una URL única, la ID de afiliado sigue siendo la misma. Cada vez que se hace clic en un enlace de afiliado, independientemente de la plataforma que esté utilizando (hablaremos sobre las compañías que le permiten inscribirse en programas de afiliado más adelante) se registra la cantidad de clics y visitantes únicos. Sin embargo, no importa cuántos clics haga en el enlace, no significa nada hasta que registre las ventas reales. En otras palabras, a diferencia de los programas de afiliación publicitaria, no lo recompensan por

dirigir el tráfico a los sitios web. De hecho, los enlaces de afiliados solo recompensan a los asociados en caso de que se realice una venta real. Esta comisión puede ser entre 1% y 10%, según el precio del producto o servicio.

El tema de los influencers puede considerarse poco ético cuando el modelo adjunto no comparte ningún interés verdadero en la causa del producto o en otro caso, cuando la empresa de marketing aplica el mismo modelo a un anuncio de una marca competidora que recibe el mismo conjunto de creencias y valores. En realidad, hay mucho dinero en publicidad digital promocional y muchas personas buscan una razón para reunir apoyo para ser parte del cambio social.

Para comenzar, necesitará una PC y / o un teléfono inteligente, un sitio web y / o un sitio web relativamente grande y, por último, una cuenta de afiliado. He enumerado estos tres criterios en orden de prioridad. Hay una gran variedad de productos disponibles en la web. Tendrá que determinar la demanda de un nicho en particular antes de decidir qué vender. Para este ejemplo, discutiremos la industria cosmética. Según los recursos que hemos recopilado en toda la industria del marketing masivo, se estima que los influenciadores de las redes sociales en promedio ganan dinero por publicar sobre un producto y / o servicio específico. La cantidad de dinero que recauda un influencer de las redes sociales se basa en el tamaño de su red. La siguiente tabla detalla el "ritmo actual" para un influyente de redes sociales en línea por cada 1000,000 seguidores.

Red Social Coste por Influencer
Instagram EUR 1,500
Snap Chat EUR 500
YouTube EUR 2,000

Además, otros factores que pueden contribuir a la determinación del precio para un influencer en las redes sociales incluyen:

- la cantidad de publicaciones de compromisos
- la cantidad de publicaciones, número de campañas,
- tipo de publicación: como (imagen, video, audio, texto)
- durancia de la publicación y / o campaña en días, semanas, meses, etc.
- la cantidad de compromiso necesaria de este influencer
- la ubicación, país, territorio y / o ubicación geográfica

Plataformas en línea como Tapinfluence y Revfluence calculan valoraciones para personas influyentes en las redes sociales. Sin embargo, algunos influenciadores de las redes sociales establecerán sus propias tarifas. Por ejemplo, las celebridades con una audiencia relativamente grande en las redes sociales pueden establecer sus propias tarifas. Kim Kardashian cobra más de EUR 250,000 por una foto de Instagram. Según la revista Forbes, los 10 principales influyentes en la industria cosmética tienen un alcance

combinado de 135 millones de seguidores repartidos en diferentes plataformas de redes sociales como seguidores de Instagram (49,157,110), Twitter (11,608,220), seguidores de Facebook (16,672,553), seguidores de YouTube (46,543,975). Además, cada una de estas diez personas influyentes cosméticas reconocidas en las redes sociales han sido participantes activos durante al menos diez años o más.

A continuación encontrará información de cada uno de estos
Los diez mejores influencers cosméticos 2019-2020

Nombre del influenciador Breve descripción

Nikkie de Jager Maquilladora holandesa 7.2 millones de seguidores en Instagram. 6.6 millones de seguidores de YouTube. Colaborando con una marca de pintalabios Ofra.

Christen Dominique Makeup Vlogger. 4 millones de seguidores en YouTube. Se asocia con L'oreal, Sephora y Urban Decay

Wayne Goss Maquillador británico. 11 millones de visitas en el tutorial de YouTube. Construye su propia marca de pinceles de maquillaje Beautylish.

Manny Gutiérrez Audiencia combinada de 7 millones entre seguidores de Instagram y YouTube. Embajador de Maybelline

Shannon Harris Nueva Zelanda vlogger. Construyó su propia marca xobeauty, vendiendo pestañas y pinceles. Se asocia con Clinique y Smashbox Cosmetics

Kandee Johnson comenzó a bloguear en 2008. 5,7 millones de seguidores entre YouTube e Instagram. Tiene su propia línea de esmaltes de uñas a la venta en Walmart y Walgreens.

Huda Kattan Famoso entre los Kardashians. Su línea de maquillaje se vende en Sephora. 26 millones de seguidores de Instagram.

Michelle Phan Suscripción caja de cosméticos Ipsy valorada en 500 millones. 1,9 millones de seguidores de Instagram. No disponible para publicidad.

Jeffree Star 4 millones de suscriptores de YouTube. Es amigo de Manny Guitierrez y tiene una línea personal de labiales líquidos.

Zoe Sugg 11,6 millones de suscriptores de YouTube. La línea de productos de belleza más vendida en una cadena llamada Super Drug en el Reino Unido. Libro de best

sellers online para niña.

Todo el mundo quiere ser un influyente en línea y tener éxito, pero aunque cualquiera puede hacer esto, no todos encontrarán el éxito, al menos no de inmediato. En cualquier caso, incluso si no se encuentra con un umbral de 100k seguidores para ganar instantáneamente miles, decenas de miles o cientos de miles de dólares, aún puede hacer ventas con una red social más pequeña siguiendo unos pocos miles de seguidores o algunos cien seguidores El objetivo, por supuesto, es VENDER. Si bien hay muchos programas de afiliación disponibles en la web, algunos de los programas de afiliación con los que he estado involucrado personalmente son Afiliados de Amazon, Rakuten LinkShare y Afiliados de CJ. Aquí pasaré por los pasos obvios de registrarse en estos programas de afiliados (que se pueden hacer a través de una búsqueda rápida en Google y registrar sus datos personales) y le contaré sobre las experiencias de los usuarios colectivos.

Los afiliados de Amazon ofrecen la mayor versatilidad en términos de inventario de productos y lo que puede vender. Después de todo, Amazon.com es la tienda de todo y tiene casi cualquier cosa, desde a-z. Entonces, si no está seguro acerca de un nicho, lo mejor sería inscribirse en Amazon Affiliates porque tendrá la libertad de vender lo que quiera. Sin embargo, Amazon es realmente estricto y, cuando se inscribe, pueden ponerlo en un período de prueba de 3 meses para vender una cierta cantidad de productos antes de que se lo considere un Afiliado de Amazon de pleno derecho. En segundo lugar, si lee los Términos y condiciones, Amazon Associates no se considera un programa de descuento y, por lo tanto, no lo recompensará si está comprando productos para usted para ganar una comisión. Por último, la desventaja es que a veces los productos están marcados, lo que significa que los enlaces de afiliados de Amazon pueden hacer que el producto sea más costoso y disuadir a los compradores que buscan una compra barata o barata.

Rakuten LinkShare es otra plataforma de marketing digital que le permite inscribirse individualmente con empresas, por supuesto, dependiendo de su nicho particular. Sí, tendrá que solicitar a cada empresa que gane una comisión por vender sus productos y ellos deberán aprobar su solicitud antes de comenzar. Por lo tanto, si tiene un sitio web sobre cosméticos o un canal de redes sociales, puede inscribirse en compañías de cosméticos en Rakuten Affiliates en la sección Salud y belleza. Algunas compañías de cosméticos que ofrecen una comisión del 10-25% son Hair.com, Mila Moursi y Shaklee. Ahora, a muchos de ustedes les puede resultar complicado tener que presentar una solicitud a cada empresa y, aunque puede ser cierto, por otro lado, tendrán la oportunidad de crear su propia cartera de productos y / o servicios para ofrecer en su sitio web. La desventaja de esta plataforma de marketing digital es que los enlaces de afiliados pueden no traducirse bien en publicaciones de redes sociales como Twitter o Facebook, lo que no genera una vista previa y un código tedioso "<a href = ...", etc., que sus seguidores generalmente no tendrán en cuenta. Estos enlaces se utilizan mejor en sitios web y blogs.

Por último, los afiliados de CJ son una empresa de publicidad en línea que se fundó

en 1998. La empresa forma parte de Publicis Group y funciona de la misma manera que la anterior al exigir a los miembros afiliados que soliciten individualmente a cada empresa. Los afiliados de CJ también tienen una gran base de clientes y le ofrecen la oportunidad de trabajar con una amplia selección de empresas. Sin embargo, CJ.com es similar a Amazon Affiliates en el sentido de que los enlaces de afiliados generados desde su cuenta en un producto específico están diseñados para HTML, Javascript y haga clic en URL (que es perfecto para las redes sociales). Además, lo que diferencia a los afiliados de CJ del resto es que le permiten crear widgets personalizados y genera el código por usted. Puede incluir widgets en su sitio web para mostrar los mejores productos a sus clientes. La desventaja de esta plataforma de marketing como afiliado es que puede terminar buscando productos, copiando y pegando el código antes de darse cuenta de que el producto ya no está disponible para la venta. Asegúrese de verificar haciendo clic en el enlace usted mismo si el producto aún está disponible para comprar antes de publicarlo.

Ahora puede sospechar de sus amigos y familiares en su red social preguntándose si alguna vez han intentado que compre un producto o servicio para ganar una comisión para ellos. Como puedes saber Antes de explicar cómo detectar un enlace de afiliado, debe comprender una conclusión y es que todos están involucrados en el marketing de afiliación de una forma u otra, por eso decidí incluir un capítulo de marketing de afiliación e influir en este libro. Ya hemos discutido las personas influyentes y cómo los vendedores afiliados ganan dinero, pero incluso los conglomerados de Internet ganan dinero con los clics de enlaces, ya sea a través de publicidad o ventas. Por ejemplo, cada vez que realice una búsqueda en Google, obtendrá resultados automáticamente. Supongamos que realiza una búsqueda en Google de cosméticos. Notarás cómo los dos primeros resultados de búsqueda son los anuncios más comunes. Si hace clic en estos enlaces y se dirige a la página, eche un vistazo a la barra de direcciones y vea si lee los servicios de Google Lead. Si la barra de direcciones de su navegador web pasa a través de Google Lead Services y termina comprando un artículo, una pequeña comisión irá a Google.

Los enlaces de afiliados son fáciles de detectar, solo vea cómo se construyen los enlaces. En términos generales, verá un enlace de afiliado al final del enlace, como linkID = Yolo5 como ejemplo, o un enlace de URL acortado, como amazon.to. Puede publicar este tipo de enlaces en el sitio de redes sociales más popular, pero no en todos, por lo que es crucial tener su propio sitio web. Alternativamente, no podrá agregar enlaces de afiliados en las publicaciones de Reddit o Instagram. Finalmente, te estarás preguntando por qué no mencioné Instagram. Instagram es una popular plataforma de redes sociales para compartir fotos y videos. Debido a que los enlaces se pueden monetizar, Instagram no permite que se agreguen enlaces en las publicaciones. Para eso, necesitaría tener una cuenta comercial de Instagram por EUR 20 / mes. Instagram solo permite agregar un enlace a su perfil, que generalmente es a un sitio web u otra página de redes sociales. Como tal, los usuarios desviados de Instagram han encontrado una forma de evitar esto y es crear una lista de enlaces en una página www.campsite.bio e incluirla en su perfil de Instagram. Para concluir, si bien estas plataformas de marketing de afiliación cuentan el número de clics en los enlaces, no especifican regiones geográficas o ubicaciones, por lo

que es útil el capítulo anterior sobre el seguimiento de enlaces. Es posible que vea enlaces abreviados como bit.ly para disfrazar enlaces de afiliados y al mismo tiempo proporcionar más investigación de mercado.

Sin duda, la capacidad de ganar dinero en línea y participar en una inversión comercial sin dinero por adelantado es absolutamente fantástica. Es más barato ejecutar una tienda en línea hoy en la web que en un proyecto de ladrillo y motor. No importa qué plataforma elijas, querrás que te vean. Muchos remitentes están ganando mucho dinero vendiendo los productos que poseen. Lo dejan en una instalación de envío local y lo envían al cliente. El producto se hace accesible a través de un enlace. En el mercado abierto hay muchas más garantías de recibir su producto. Sin embargo, en el mercado negro es posible que su capacidad para quejarse sea inútil. En otras palabras, no existe un departamento de rendición de cuentas porque las personas a cargo no quieren ser consideradas responsables y, por lo tanto, no se identifican. Una especie de Atrápame si puedes vibrar. Tendrás que ejercitar mucho más músculo en el mercado negro que en el mercado abierto, ya que no hay atractivo para las autoridades en el primero. ¿Por qué la privacidad es algo bueno para las personas buenas y no algo bueno para las personas malas? Presumiblemente, veamos el anonimato en la web como un concepto.

Anonimato en la web

La privacidad en línea es un tema de creciente preocupación debido a los peligros manifestados de hacer un seguimiento de su ubicación (dirección IP) y / o información confidencial (como: cuenta bancaria, contraseñas, etc.) robada. Como tal, las medidas de ciberseguridad a menudo se emplean para agregar una capa de protección a los usuarios de computadoras y dispositivos inteligentes. En este capítulo, hablaremos sobre los diferentes tipos de capas de ciberseguridad que podemos agregar a nuestros dispositivos, entenderemos cómo podemos volvernos vulnerables sin ellos y por qué más los necesitamos. A medida que avanzamos hacia el futuro, las personas dependen cada vez más de establecer una conexión a Internet con sus dispositivos. De hecho, como hemos dicho de manera similar en el primer capítulo en un futuro cercano o tardío, todos los tipos de dispositivos electrónicos se conectarán a Internet, incluidos nuestros electrodomésticos más comunes: refrigeradores, lavadoras, secadoras, cafeteras, etc. Demanda de conectividad a Internet Ciertamente está creciendo y, por lo tanto, la necesidad de proteger nuestra red doméstica y comercial es crucial. En 2004, el mercado global de seguridad cibernética se valoró en EUR 3.5 mil millones; más de una década más tarde en 2017 alcanzó más de EUR 120 mil millones. Según Statista, se espera que el mercado de seguridad global alcance los EUR 250 mil millones para 2023.

Para comenzar, Internet es un vasto recurso para la información, el intercambio de archivos, la comunicación y la realización de transacciones comerciales. Podría decirse que si no fuera por nuestros intentos de apaciguar muchas de nuestras curiosidades en busca de información y otro tipo de contenido en línea, es posible que nunca hubiéramos puesto en riesgo nuestra ciberseguridad en primer lugar. Desafortunadamente, los

usuarios se intrigan en la búsqueda de información, hacen clic en enlaces sospechosos a páginas web y / o descargan archivos corruptos y, por lo tanto, corren el riesgo de ataques cibernéticos y divulgan su información personal. Mantener el anonimato viable es tan importante que incluso los hackers no quieren ser identificados. Principalmente, los piratas informáticos no quieren ser rastreados porque si son encontrados serán arrestados y acusados por sus crímenes. En 2017, más de 143 millones de estadounidenses fueron víctimas de delitos cibernéticos. Hoy, los cinco principales delitos de ciberseguridad son malware, fraude con tarjetas de crédito y débito, violaciones de datos, contraseñas comprometidas y acceso no autorizado a las redes sociales. Puede que se pregunte por qué piratean los hackers. Bueno, los piratas informáticos pueden piratear por una serie de razones, como exponer una vulnerabilidad en un sistema (Pen Tester), por placer (schadenfreude) y / o ganar y, simplemente, porque pueden.

Hay piratas informáticos que pueden disfrutar arruinando la vida de una persona, ya sea por venganza o por ganancia personal. En última instancia, cuando la relación es personal, puede ser más doloroso ser engañado o estafado de alguna manera. ¿Alguien ha estado tan enojado contigo por decepcionarlo? ¿Alguna vez alguien te ha buscado venganza? ¿O ha tenido ganas de vengarse de él / ella? Se ha dicho que la venganza puede nublar tu juicio. Como testimonio de fe, la Biblia ordena a los seguidores que NO busquen venganza. Después de todo, en tu intento de lastimar a alguien, podrías terminar lastimándote a ti mismo. En el primer libro Cibercrimen: las amenazas al navegar en Internet y las redes sociales, discutimos el mercado negro y cómo puedes contratar a un hacker para destruir la vida de alguien. Tenga en cuenta que no apruebo esta actividad, pero independientemente de mis creencias, se hace y se puede hacer. Un hacker vive una doble vida. Un hacker puede ser cualquiera. Un hacker puede ser alguien que conoces en la calle, tu cartero, un tendero local, un compañero de clase o un profesor. Esta estima me recuerda a la popular película Matrix, donde Neo, también conocido como Thomas A. Anderson, vivió una doble vida, una como programador de computadoras en una oficina corporativa y la otra como un cibercriminal clandestino.

En retrospectiva, la historia de Joe Good es un ejemplo perfecto de cómo alguien cercano a ti también puede ser un hacker y arruinar tu vida. Joe Good fue un gerente de reclamos de seguros que entrenó al equipo de fútbol de su hijo pro bono. Un día, conoció a una mujer (Tawny Blazejowski) de quien se enamoró en uno de los juegos. Como la

mayoría de las parejas de hoy, publicaron su actividad en Facebook. Su relación se volvió seria que después de dos años juntos estaban comprometidos. Sin embargo, cuando Joe no pudo comprometerse a fijar una fecha, Tawny ejecutó un plan de venganza que comenzó con ella privándolo de cosas como unas vacaciones que habían planeado y luego amenazó verbalmente con "arruinarlo". Tawny comenzó pirateando su cuenta de correo electrónico de Yahoo, luego le envió por correo electrónico fotos íntimas de él que compartieron con su jefe y colegas. Tawny no se detuvo allí, luego envió juguetes sexuales y condones a través de FedEx a su compañía. Además, trató de incriminarlo por abusar físicamente de ella, lo acusó de incesto de tener relaciones sexuales con su propia hija y de ser un pedófilo de tener relaciones sexuales con niñas menores de edad al denunciarlo a Crime Stoppers. Cuando Tawny terminó, lo hizo arrestar tres veces, despedirlo de su trabajo de ingresos de seis cifras y escribir cartas amenazadoras a los amigos y la nueva novia de Joe. Al final, Tawny fue atrapada, mantuvo un registro diario de todas sus actividades que fue recuperado por la policía junto con su número de teléfono que fue rastreado y utilizado para engañar a la policía al escribir sus informes. Finalmente, Tawny fue sentenciada a 9 años de cárcel más 2 años de arresto domiciliario.

Discutiremos algunas de las capas de seguridad que incluso algunos hackers pueden usar para mantener su identidad en secreto. No importa si es un hacker o no, es aconsejable mantener su identidad y ubicación discretas para evitar ser blanco de daños. Tenga en cuenta que no existe una estrategia a prueba de tontos para ser anónimo en la web. Incluso las capas de cifrado se pueden descifrar, pero pueden dificultar la comprensión de la información al codificarla y hacerla ininteligible. No obstante, ofreceremos algunas recomendaciones que serán útiles para mantener su identidad en secreto para cualquier propósito. En palabras del escritor romano clásico Cornelius Nepos, "Después de la oscuridad viene la luz".

TOR

¿Qué es TOR?

El proyecto Tor es una organización sin fines de lucro que proporciona una red mundial gratuita y de código abierto que permite la privacidad y la comunicación en línea. Tor es un acrónimo de The Onion Router. Inicialmente desarrollado por la Marina de los EE. UU., Ahora es utilizado principalmente por muchas personas para navegar en la web de forma anónima. Para la mayoría, Tor ha demostrado ser eficiente. Inhabilita su ubicación y bloquea las solicitudes de conexión entre servidores calculadas a su máquina que permiten al gobierno rastrear su historial web. El nombre cebolla se deriva quizás del hecho de que hay varias capas de cifrado proporcionadas en la experiencia, de forma similar a cómo hay muchas capas en la "cebolla" vegetal. No obstante, lo que hace Tor es ofrecer un conjunto de retransmisiones para rebotar su tráfico web para eludirlo a sí mismo a fin de no revelar información a estas solicitudes durante el escaneo y monitoreo habitual de los proveedores de servicios de Internet. El software enmascara la dirección IP cuando usa el navegador mientras visita sitios web y servicios cuestionables que pueden estar restringidos por las leyes de censura del gobierno. Sin embargo, si alguna vez inicia sesión en su cuenta, aunque sea desde una cuenta de Google o Facebook, puede comprometer su identidad al compartir que ha iniciado sesión en un dispositivo en particular utilizando una plataforma específica. ¿Recuerdas que discutimos en un capítulo anterior cómo se puede usar el enmascaramiento de URL para rastrear tu IP y / o ubicación? También se puede usar para detectar su sistema operativo y navegador web. Entonces, si tuviera que hacer clic en un enlace e iniciar sesión con su nombre de cuenta y contraseña, en este caso, sería inevitable que los intentos de Tor para protegerlo se vuelvan inútiles. Parte de la responsabilidad recae en las prácticas informáticas de un individuo. También hay complementos desinstalados como Flash, un reproductor de ondas de choque de Adobe que requiere que instales Javascript, un lenguaje de programación que escribe applets en tu máquina. Sin él, es posible que no pueda ver cierto contenido en un navegador determinado. Por lo tanto, dependiendo de sus actividades, puede ser vital preinstalar el software, sin embargo, debe hacerlo bajo su propio riesgo.

La cuestión de Tor es un tema controvertido dependiendo de quién lo usa y cómo se aplica. Tor puede ser utilizado por cyberthugs y comerciantes del mercado negro para permanecer en el anonimato en la web. En Internet, el mercado negro plantea una serie de obstáculos para la policía y los federales que buscan poner fin a las actividades ilícitas en la web. La famosa Ruta de la Seda (un sitio web para comprar drogas ilegales) funcionaba en un dominio impulsado por Tor. El sitio web requería que los usuarios crearan un nombre de cuenta y contraseña. Como una capa adicional de contraseguridad cibernética, los proveedores aceptan estrictamente el pago en forma de Bitcoin. Una lección fundamental es que tanto el Wi-Fi como el navegador web juegan su parte para

proporcionarle el anonimato mientras está en la web. Para proporcionar una prueba de concepto, el desarrollador de la Ruta de la Seda, Ross William Ulbricht, fue arrestado en la sucursal de la Biblioteca Pública de Glen Park en San Francisco, California, en octubre. 1 de 2013 porque se olvidó de ponerle valor al primero. Ross operaba en el sitio Silk Road bajo el alias "Dread Pirate Roberts", aunque pudo haber estado usando su computadora portátil personal en la biblioteca, todavía estaba en una conexión Wi-Fi financiada por el público (dólares de impuestos), monitoreada y regulado por el gobierno. En primer lugar, permítanme decir que cada vez que acceden a una computadora o conexión Wi-Fi en una biblioteca pública o empresa, hay ciertas condiciones que deben cumplir, reglas o advertencias si lo desean, a lo que deben dar su consentimiento para poder para acceder a la web. Antes de establecer una conexión a Internet, debe aceptar los Términos y condiciones que pueden poner su uso en restricciones de tiempo de media hora a una hora y que consiste en aceptar no realizar actividades ilícitas mientras se encuentre en la red Wi-Fi correspondiente. Como veremos en la siguiente sección, la configuración de una VPN puede ayudarlo a agregar otra capa de seguridad en línea, pero nuevamente, estas redes pueden restringir el acceso si está utilizando alguna de estas herramientas.

Para continuar, todavía hay muchos sitios web oscuros en la web similares a Silk Road que comparten un dominio web impulsado por Tor. Estos sitios a menudo están encriptados y son direcciones web ininteligibles que funcionan a través de una serie de sitios espejo que a menudo dejan de funcionar a medida que operan continuamente al recorrer páginas web alternativas. Uno de los peligros inherentes de comprar en este tipo de sitios web además del hecho de que está cometiendo un delito es que debido a que está pagando en Bitcoin u otra criptomoneda, no tiene garantía de devolución de dinero tan pronto como envíe BTC de su billetera virtual. Por ejemplo, cuando envía BTC a la dirección incorrecta, se dice que los fondos se pierden para siempre. Alternativamente, si paga con Bitcoin por un artículo que nunca recibe, ¿a quién podría quejarse por ser estafado mientras intenta comprar bienes y / o servicios ilegales? Bitcoin no es una moneda encomendada por el gobierno. No conocemos la identidad de Satoshi Nakamoto. Los dólares están asegurados por la plena fe del Gobierno Federal y reconocidos como moneda de curso legal. En caso de que desplace la criptografía, no tiene a dónde dirigir su reclamo ni legitimidad para recuperar pérdidas financieras cuando intercambia Bitcoin. Los delincuentes pueden querer robar su dinero y venderle productos ilegales, pero la razón por la que Tor no se ha cerrado todavía no es tanto que los delincuentes quieran su dinero y también utilicen Tor para navegar por la web de forma anónima, sino que es que las empresas y el gobierno también quiere tu dinero. Un grupo de empresas y el Gobierno quieren saber qué está buscando en Internet para saber qué anuncios pueden usar para la segmentación, dirigidos a posibles clientes y generando ingresos por ventas. El hecho es que las personas tienen derecho a la privacidad y a rechazar solicitudes. Tor todavía está llevando a cabo sus operaciones de investigación y desarrollo, no es un método infalible para navegar en la web de forma anónima, pero es una herramienta importante. En las siguientes dos secciones discutiremos etapas adicionales, que pueden ayudarlo a implementar más capas de encriptación y seguridad para navegar por Internet de forma un poco más privada.

VPN

Muchas personas quieren poder navegar en Internet sin que los mismos anuncios los sigan a través de diferentes sitios web y contenido visual en línea. El uso de Wi-Fi público o puntos calientes puede presentar peligros porque, además de estas conexiones monitoreadas por el host, también son redes compartidas con otros usuarios que pueden acceder a su dispositivo de forma remota. Una red privada virtual o VPN ofrece varias capas de cifrado y le permite establecer una conexión segura a otra red a través de Internet. Oculta su ubicación y dirección IP. En primer lugar, hay un par de beneficios adicionales con el uso de una VPN. Podemos usar una VPN para acceder a contenido específico de la región. Este aspecto importante ayuda a los viajeros que pueden estar fuera del país a acceder a contenido disponible solo en los Estados Unidos, pero también ayuda al usuario de VPN a obtener acceso a contenido sin censura en sitios web alojados por otros países que no están disponibles en los Estados Unidos. Si, por ejemplo, deseas ver Netflix, Hulu, HBO mientras te encuentres en el extranjero, es posible que se le solicite tu cuenta de transmisión de vídeo y que no sea accesible desde fuera de los Estados Unidos y eso niega los servicios de soporte de base de nube mientras tu señal permanece lejos de tus redes de comunicación. Sin embargo, para acceder mejor a este contenido, tendrás que ser un mago y ejecutar un poco de magia informática todo lo que necesitas hacer es ajustar tu ubicación geográfica en el sistema de la VPN. Normalmente, puedes disfrazar tu ubicación digital en EE. UU a diferentes países a través del mundo. Un VPN es una red privada de servicio pagado que normalmente debes abonar dinero por el privilegio de estar protegido en línea. Hay pocos servicios de VPN gratuitos, pero ninguno se recomienda, ya que todos se ejecutan en los propios anuncios, pueden ser defectuosos y ofrecen una protección limitada. Realmente, sería contrario al todo propósito tener un

servicio de red VPN (no pagado) ya que este se ejecute con anuncios.

Ahora, cuando decidas qué suscripción de red VPN debes encontrar las que requieran hardware. Descarga un servicio de red VPN para mantenerte protegido en línea teniendo en cuenta que, si bien cuando se conecta a redes Wi-Fi en aeropuertos, bibliotecas y otras instalaciones públicas, la conexión a Internet puede verse interrumpida. Existen políticas burocráticas existentes que han requerido un poco de "transparencia", una moción basada en la iniciativa para combatir el ciberterrorismo. En ese caso, el uso de la red VPN puede deshabilitar su conexión Wi-Fi en lugares públicos. Elije una suscripción de red VPN que sea rentable para ti. Anualmente, esta red VPN generalmente cuesta alrededor de EUR 30 a EUR 100 dependiendo del proveedor de servicios con el que elijas suscribirte y la cantidad de dispositivos que desea agrupar en su plan de protección. Algunas de las VPN que recomendamos son Kaspersky, Norton VPN, TorVPN y AVG VPN. Hay diferentes descargas de VPN disponibles para PC: Microsoft, Mac, Linux y Smart Phones: Android e iOs. Mientras usas una red VPN, también puede hacer algunas compras en línea y comprar productos específicos de la región a precios disponibles solo en tu país y en la misma moneda. Si usaras el navegador Tor y una red VPN, piense en la cantidad de capas de seguridad que está enmascarando en tu dispositivo, suponiendo que también tenga un antivirus. Actualiza y cambia la ubicación operativa de tu red VPN para poder reforzar tu anonimato en la web en caso de que tu dirección IP aparezca en la lista negra. Esto puede suceder cuando ciertos mecanismos de control de acceso buscan pasar y acceder a información para verificar su identidad. Información que se atribuye a direcciones de correo electrónico, nombre de usuario y contraseñas, nombres de dominio, dirección IP, ubicación, etc. Si permites que tu navegador detecte su ubicación, está comprometiendo tu privacidad, por lo que no tendría sentido usar la red VPN. Por último, si otro usuario está conectado a la misma red LAN local que tu, aún puede rastrearlo a través de otros medios. Para estar seguro, asegúrese de establecer configuraciones privadas en la conexión de red de tu dispositivo y proteger con contraseña tus dispositivos también.

(Virtual Box) Caja virtual

Finalmente, ahora que hemos discutido dos instrumentos que se utilizan para mantener el anonimato en la web, como el navegador TOR y la VPN, revisaremos Virtual Box. ¿Qué es el VBox? VBox o Virtual Box es una máquina virtual que se ejecuta en el sistema operativo de su computadora, como: Windows, MacOS, Linux y Solaris. Está escrito en lenguaje de programación de computadora C, C ++, x86. Virtual Box es un paquete de software gratuito y de código abierto. Inicialmente fue lanzado en enero. 17

de 2007 y desarrollado por Oracle Corporation. Esta herramienta ofrece el beneficio de probar aplicaciones en un entorno controlado. Cuando configura Virtual Box, asigna la CPU y la cantidad de RAM y espacio en disco para usar. Dejas de lado la capacidad de memoria para la máquina virtual que toma su propia dirección IP. En combinación con un navegador sin seguimiento como Tor, una VPN y una máquina virtual, estaríamos empleando tres escalas de ciberseguridad para mantener el anonimato en Internet. Debería descargar Ubuntu en Windows para configurar la configuración. En segundo lugar, es necesario crear un nombre de usuario y contraseña para conectarse a su dispositivo, similar al que usa para iniciar sesión en su PC cada vez que enciende su computadora. VBox también es útil en términos de ocultar sus documentos. Puede optar por mantener sus archivos ocultos y accesibles solo a través de su VBox o compartir permisos y acceso con todo el sistema. El proceso de descarga y configuración puede llevar un tiempo. Una vez que esté completo, verá un escritorio separado ejecutándose en una ventana de su PC. Maximice esta ventana configurándola en Pantalla completa y verá aplicaciones de escritorio precargadas en el nuevo escritorio de su máquina virtual. También puede descargar aplicaciones adicionales de la App Store para ejecutar funciones alternativas. Virtual Box es una herramienta que coloca al usuario de la computadora bajo otra capa de seguridad. Es una máquina virtual dentro de una máquina física. Esencialmente, es completamente metafísico.

Los pros y los contras de usar un Virtual Box son simples. En primer lugar, cuando usa su máquina virtual, su configuración de red se establece automáticamente en NAT, lo que significa que los recursos en su red no podrán ver qué dispositivo está usando. Al asignar la cantidad de RAM y espacio en disco para su máquina virtual, puede descubrir que tendrá que establecer límites. Cuanto más baja sea la memoria de su máquina virtual, menor será la calidad y eficiencia de su sistema operativo. Estas características pueden atribuirse a la velocidad de procesamiento, píxeles y resolución. Virtual Box actualmente se ejecuta en versiones de 32 bits y 64 bits. Tenga en cuenta que la correlación entre VBox y su PC es una simbiosis donde estos sistemas operativos son interdependientes. Debido a que el VBox se integra con el sistema operativo del host, también depende de la relación con el sistema operativo del host, las capacidades de Virtual Box no pueden superar las de los hosts y, por lo tanto, ambas comparten exactamente las mismas debilidades. En resumen, hemos aprendido a lo largo de este capítulo la importancia de utilizar Tor para cifrar datos mediante la conexión a través de diferentes relés y el borrado de la información de caché que dificulta el seguimiento de los usuarios que navegan por Internet en un navegador específico. Posteriormente, se necesita una VPN para ocultar su ubicación y dirección IP y, por último, Virtual Box es una herramienta utilizada para ocultar la verdadera identidad de su dispositivo debido al hecho de que está utilizando un sistema operativo cuando está en una máquina virtual.

"He estado usando Coin base, lo que hace que sea realmente fácil y seguro comprar, vender y almacenar moneda digital (como Bitcoin).

Regístrese ahora y obtenga $ 10 de Bitcoin gratis cuando compre o venda al menos $ 100 de moneda digital ".

Reclama tu invitación ahora:Criptomonedas en el Mercado Virtual

Las criptomonedas proporcionan un medio de intercambio virtual que se aprovecha de la tecnología blockchain para obtener descentralización, transparencia y un control fijo de los activos. Las criptomonedas están descentralizadas porque no están reguladas por ninguna autoridad central o banco y son teóricamente inmunes al control del gobierno. Sin embargo, hay muchos gobiernos estatales y federales que han promulgado leyes contra Bitcoin y otras criptomonedas. Dependiendo de dónde resida en los Estados Unidos y otras partes del mundo, puede estar sujeto a ciertas restricciones y se le impedirá tener criptomonedas. Por ejemplo, es posible que no pueda invertir en criptomonedas si es residente de Nueva York. La Comisión de Comercio de Futuros de Productos Básicos de los Banqueros y CFTC del estado ha tomado medidas para mantener alejadas a las criptomonedas debido a su volatilidad; presentación de

demandas e imposición de estrictas regulaciones financieras. De hecho, su cuenta bancaria en Nueva York puede cerrarse si se le encuentra tratando con Bitcoin et al. Por un lado, Bitcoin tiene muchos beneficios que discutiremos en esta sección, sin embargo, es un tema que ha ganado mucha agitación política desde el lanzamiento al mercado de la moneda virtual en 2009. En esta etapa, ha sido más Han pasado diez años desde la aparición de Bitcoin y hoy en día muchas otras criptomonedas siguen al líder. Hay muchas aspersiones emitidas en Bitcoin y otras criptomonedas, ya que la forma de pago se puede usar para comprar bienes y servicios ilegales como drogas, armas y sicarios. Bitcoin se ve obstaculizado por las autoridades bajo la presunción de que puede proporcionar un canal para el lavado de dinero y el fraude, especialmente en los casos en los que no informa al IRS sus ganancias. El presidente Trump ha prometido prohibir Bitcoin cuando el precio alcance los EUR 100,000. Actualmente, hay 21 millones de Bitcoins en circulación y si el precio de un solo Bitcoin llegara a EUR 100,000 (como pronostica amenazantemente el presidente Trump) la capitalización de mercado equivaldría a 2,1 billones de dólares. No está claro si esta ley se implementará durante su próximo mandato o el de un futuro presidente. No obstante, se cree que el futuro de Bitcoin es optimista, ya que continuará aumentando en valor ofreciendo fallas de ganancias a los accionistas a medida que fluctúa el mercado. En cualquier caso, en los últimos años hemos visto que el precio de Bitcoin fluctúa entre EUR 7,000 y EUR 20,000 dólares. Alternativamente, en esta sección cubriremos cómo comenzar a invertir en criptomonedas creando su propia billetera virtual, aprenda cómo puede obtener ganancias comprando y vendiendo criptomonedas, así como extrayendo y ganando dinero con criptomonedas que generan dividendos.

Comencemos con la configuración de su billetera virtual. Para mantener cualquier tipo de criptomoneda, debe crear una billetera virtual. Hay varias plataformas disponibles hoy en día que pueden usarse tanto en su PC como en su dispositivo de teléfono inteligente para hacer esto. Tres billeteras virtuales utilizadas por muchos otros inversores en criptomonedas son Coin base, eToro y Kraken. Para suscribirse a estas plataformas, deberá utilizar su identidad real, datos personales, información de contacto y, una vez más, deberá presentar documentos legales como su licencia de conducir o pasaporte para verificar su identidad. Así es como también pueden determinar en qué estado vive y si está sujeto a ciertas restricciones por parte del estado. Sin verificar su identidad, no podrá comenzar a operar en su cuenta. Adversamente, compartiré un hecho que la mayoría de la gente probablemente no sabía sobre el proceso de registro. Comencé a aprender sobre Bitcoin en 2017. Cuando busqué crear mi billetera virtual por primera vez, encontré algunas dificultades porque no podía verificar mi cuenta debido a que estaba estudiando en el extranjero en una Escuela Europea de Negocios en Madrid, España. Seguí recibiendo errores que pueden no verificarse debido a que mi dirección IP no coincidía con la ubicación de los documentos que presenté. Irónicamente, ni siquiera un servicio VPN podría haberme ayudado a superar este dilema. Sin embargo, en el momento en que regresé a los Estados Unidos, creé mi billetera virtual y he estado invirtiendo desde entonces. Una vez que se verifique su billetera virtual, puede comenzar a comprar y vender criptomonedas sin importar en qué parte del mundo se encuentre. El

tipo de billetera virtual que cree depende completamente de usted. Es posible que desee decidir crear una cuenta en una plataforma que cobra la menor cantidad de tarifas que puede depender de sus preferencias, pero también puede tener un riesgo adicional. La base de monedas cobra entre 1% y 3% de los depósitos y retiros, eToro cobra una tarifa fija de EUR 25 por retiros con un retiro mínimo de EUR 50 y Kraken cobra tarifas de hasta 0.26%. Sin embargo, si bien Kraken puede cobrar la menor cantidad de tarifas en su intercambio, puede haber ramificaciones con algunas de sus características. Kraken tiene un multiplicador que le permite invertir básicamente en criptomonedas a crédito. Entonces, solo tiene EUR 100 para invertir en su cuenta de Kraken, pero le gustaría invertir EUR 500. Si el precio de Bitcoin sube, entonces usted obtuvo grandes ganancias y puede pagar Kraken, pero si el precio de Bitcoin baja, entonces no solo le debe EUR 400 a Kraken, sino que también recibirá menos "Satoshis" (una denominación menor para Bitcoin) por la cantidad de dólares que gasta. En segundo lugar, con respecto a eToro, es obvio que por pequeñas cantidades de dinero no querrá pagar una tarifa fija de EUR 25, incluso si una de sus características especiales es que puede copiar la actividad comercial de inversores prominentes y exitosos. Se dice que Coinbase es la plataforma más amigable para principiantes para el comercio de criptomonedas.

"He estado usando Coin base, lo que hace que sea realmente fácil y seguro comprar, vender y almacenar moneda digital (como Bitcoin).

Regístrese ahora y obtenga $ 10 de Bitcoin gratis cuando compre o venda al menos $ 100 de moneda digital ".

Reclama tu invitación ahora:
https://www.coinbase.com/join/frias_pv?src=android-email-invite

"Déjame saber si necesitas ayuda."

A continuación, me gustaría analizar los tipos de criptomonedas disponibles en Coinbase y cómo puede operar en la plataforma. Una vez que haya verificado su identidad y los detalles de su cuenta bancaria para depósitos y retiros, puede comenzar a operar en el sitio. Tenga en cuenta que usar su cuenta corriente puede ayudarlo a ahorrar hasta un 50% en tarifas. Abra la pestaña Precios y allí podrá ver una lista de las criptomonedas disponibles para el comercio. Hay docenas de criptomonedas en la base de monedas y aún más de ellas que actualmente no se comercializan en la plataforma. Existe un peligro con las criptomonedas copycat, por así decirlo, que intentan fabricar el valor de su moneda para obtener dinero de las víctimas desprevenidas. Si una criptomoneda no figura en la base de Coin, recomendaría que se mantenga alejado de ella, ya que puede considerarse inútil. Muchas personas solo aceptan el pago en un

número limitado de criptomonedas de todos modos, con Bitcoin obviamente siendo el primero, Bitcoin Cash, Ethereum, Litecoin, Dash y Monero, entre otros. En este momento, hay dos criptomonedas disponibles en Coinbase que le permitirán obtener recompensas de los interesados y bajas tasas de interés. El USDC es una criptomoneda desarrollada por el consorcio CENTER que iguala su inversión dólar por dólar y produce una tasa de interés de 1.25% APY. Si tiene el dinero para una inversión considerable a largo plazo, le recomendaría que lo coloque en USDC ya que no hay ningún riesgo involucrado. Además, Tezos es otra criptomoneda con un precio de poco más de un dólar, pero le ofrece recompensas de hasta 5.55%. Coinbase tomará un pequeño porcentaje de las recompensas de participación, así como las comisiones de los depósitos realizados desde su cuenta bancaria y cuando venda su criptomoneda nuevamente en efectivo, pero no le cobrarán tarifas si convierte su criptomoneda en otra criptomoneda. Le permite comprar $ 40 de Dash y luego el precio sube a $ 50, dejándolo con una ganancia de $ 10, puede optar por convertir sus $ 50 completos o solo una fracción de su saldo en otra criptomoneda como Bitcoin Cash, por ejemplo, sin tener que pagar tarifas. Además, otra opción para que usted invierta en criptomonedas sin tener que usar sus dólares reales sería extraer Bitcoin y otras criptomonedas. Este proceso puede ayudarlo a evitar correr el riesgo de guardar sus dólares en estas cuentas de inversión, pero tampoco incurrirá en ninguna tarifa al recibir Bitcoin y otras criptomonedas. En otras palabras, se cobran tarifas por los depósitos en su cuenta de Coinbase que paga con su cuenta bancaria y no si recibe BTC et al. de cuentas externas Sin embargo, una vez que retire Bitcoins de su billetera virtual, también tendrá que pagar una pequeña tarifa.

¿Qué es blockchain?

Blockchain es una tecnología segura que se emplea para verificar transacciones digitales. Blockchain se popularizó por primera vez como una forma de administrar Bitcoin. No puede ser violado. Si bien la información se almacena en una base de datos pública y cualquiera puede ver el contenido de la red blockchain, las partes involucradas permanecen sin identificar agregando un elemento de ciberseguridad para los usuarios. Blockchain almacena información como sellos de fecha y hora, cantidades en dólares y una firma digital. En un ejemplo, podríamos tener dos personas participando en una transacción en línea. La cadena de bloques recibe todos sus datos, excepto las identidades de los usuarios que transmiten la información a través de una red de computadoras que utilizan la potencia de procesamiento para verificar la transacción. El propósito del proceso de verificación es mantener un registro contable de todos los bitcoins en circulación y asegurar que nadie bitcoin se use dos veces. Recuerde que solo hay 21 millones de Bitcoins y, aunque el valor de la criptomoneda ha demostrado sesgar miles de dólares en los últimos años, la cantidad de bitcoins es fija.

¿Por qué el anonimato de Bitcoin se ve negativamente y por qué no más personas lo han adoptado como medio de intercambio?

Las instituciones bancarias y las autoridades han objetivado a Bitcoin como una herramienta para el lavado de dinero y han difamado su uso. En 2017, el CEO de JP Morgan, Jamie Dimon, calificó a Bitcoin de "fraude". Quizás la principal queja para las autoridades no es que Bitcoin sea un bien intangible, ya que los bancos tienden a mover cientos de miles de millones de dólares en transacciones digitales en un día determinado, sino más bien que Bitcoin es una moneda descentralizada totalmente compatible con una red P2P-Peer to Peer. En otras palabras, las autoridades gubernamentales pueden hacer poco o nada para confiscar una criptomoneda no regulada. Esencialmente, este paradigma es la economía de laissez-faire ejemplificada. Cada año, el gobierno de los Estados Unidos confisca miles de millones de dólares en activos de delincuentes. En la historia de Ross Ulbricht, autor intelectual del mercado de drogas en línea Silk Road, el FBI logró incautarle 600,000 BTC (una cantidad separada de los 26,000 BTC que quedan en una cuenta de Escrow) pero no pueden acceder a la billetera virtual porque es encriptado Podría decirse que si este evento no hubiera sucedido, el valor de Bitcoin no sería lo que es hoy o habría sido prohibido. A fin de cuentas, este movimiento fue un paso más allá para que la criptomoneda ganara legitimidad. En cualquier caso, a fines de 2019, el presidente Trump prometió prohibir Bitcoin una vez que el valor de la criptomoneda alcanzara los $ 100,000. De hecho, la volatilidad del mercado del bitcoin ha sido motivo de preocupación. Por último, estas fluctuaciones de precios son la razón por la cual la mayoría de las empresas aún no aceptan Bitcoin como forma de pago. Al final, un dólar es un dólar, pero un Bitcoin puede valer $ 8,000 hoy y la próxima semana el valor podría aumentar o disminuir. Se sabe que Bitcoin cambia hasta un 3% en solo unos minutos o más. Para los dueños de negocios, esto presenta un riesgo innecesario contra sus márgenes de ganancia cuando se trata de la venta de bienes tangibles.

Cripto minero

Hasta ahora, hemos discutido cierta información sobre Bitcoin y probablemente ya se esté preguntando cómo adquirir Bitcoins o al menos una fracción. Los bitcoins se dividen en Satoshis. Hay 1,000,000 de Satoshis en un Bitcoin. En esta sección, hablaremos sobre cómo obtener skin en el juego. Por supuesto, Bitcoins se puede comprar a través de cualquiera de las plataformas de negociación que hemos visto en este libro, así como en algunas otras, pero Bitcoin no se puede considerar formalmente como dinero o medio de intercambio a menos que las personas puedan ganar eso. Muchas personas están ganando criptomonedas a través de la minería, sin embargo, en esta etapa, la práctica está lejos de ser generalizada. La minería de criptomonedas es el proceso de calcular un valor específico que completará un "bloque" en la cadena de bloques, una vez que se resuelve ese bloque, los mineros son recompensados con Satoshis. Estas recompensas suelen ser pequeñas. De hecho, no espere obtener una cantidad significativa de ingresos a través de la minería de criptomonedas a menos que esté dispuesto a invertir $ 3500- $ 5000 en costos de equipo o hardware por adelantado. Hay una serie de aplicaciones y software disponibles que permiten a cualquier persona comenzar con la minería de criptomonedas con solo $ 0 utilizando su teléfono inteligente o computadora. Incluiremos dónde obtener estas aplicaciones y herramientas que lo ayudarán a ganar dinero todos los días para mantener en su propia alcancía virtual personal. A continuación hay algunos enlaces para ganar BTC Satoshis, ETH Gwei LTC Litoshis y BCH Satoshi. Descargue estas aplicaciones en su dispositivo y gane las siguientes criptomonedas.

Aplicaciones para descargar a su dispositivo de teléfono inteligente
Free Bitcoin Cash
Free Litecoin
Cointiply

Tenga en cuenta que el valor de estas monedas puede aumentar o disminuir sustancialmente a veces. Las conversiones de moneda entre estas criptomonedas y EUR se dan (como una fracción de un número entero) considerando cuánto valen hoy. Por supuesto, puedes ganar más dinero invitando a amigos.

Además, las aplicaciones número 1, 2 y 4 son de una aplicación Gaming and Chance que incluye girar en un tablero de números. El número 4 es la aplicación más estricta

porque requiere que los jugadores usen ingresar una frase CATPCHA, mientras que los dos primeros solo requieren que toques algunas veces. Posteriormente, la aplicación número 3 es un juego que requerirá que seas más interactivo para ganar recompensas. A fin de cuentas, la aplicación número 4 es el significado más gratificante que le permite ganar la mayor cantidad de dinero de los otros tres. Solo puede retirar efectivo después de 35,000 monedas, que es 0.00035 BTC, que es de aproximadamente EUR 3.50, y siempre que deje el saldo en la cuenta, le permite ganar un 5% de interés cada año. La aplicación número 1 y 2 es un juego que te permite ganar cada hora un número X de Litoshi o BCH Satoshi con un umbral mínimo de 40,000 Litoshi, lo mismo que EUR 0.02 y 10,000 BCH, que es EUR 0.032 Satoshi para cobrar. Además, garantizan el pago todos los martes a sus billeteras virtuales. Describiría la APP Número 3 como un juego similar a Candy Crush, pero en lugar de caramelos, estás bloqueando bloques de criptomonedas para simular la cadena de bloques. Estos pequeños bloques incluyen sus logotipos. Para este juego, hay un mínimo de 100 GWEI, la unidad GWEI es una fracción de Ethereum que puedes ganar simplemente jugando este juego. Sin embargo, solo puede cobrar una vez cada dos días. La cantidad máxima para retirar incluye 300,000 GWEI, que es el equivalente a 0.0000003 ETH, que es aproximadamente EUR 0,04.

Si bien estas aplicaciones humildes son de uso legítimo, el aspecto negativo de buscar otras aplicaciones y software de criptomonedas en Internet es que corre el riesgo de encontrar estafas y virus, ya que muchos de esos archivos que puede intentar descargar están dañados. Alternativamente, si decide minar a través de aplicaciones y software, sus ganancias honestas serían equivalentes a ganar unos centavos por día, mientras que muchos mineros avanzados de criptomonedas con una importante inversión en hardware informan que ganan EUR 50- EUR 100 por día.

Hablemos sobre qué tipo de hardware se necesita y cómo se usa. Muchos de estos programas y grupos de minería requieren que obtenga una tarjeta gráfica 4 ASIC, Nvidia y AMD Radeon con suficiente potencia de procesamiento para ejecutar estos programas. También necesitará una conexión a Internet de alta velocidad confiable ya que toda la operación debe estar en línea para poder obtener los beneficios. El Antminer S9 es una de las mejores piezas de hardware en el mercado en el momento de escribir este artículo y se dice que es el hardware más eficiente para extraer criptomonedas. Tenga en cuenta que una vez que compre el equipo necesario para extraer, tendrá que mantenerlo en un lugar fresco, posiblemente con aire acondicionado, ya que estos dispositivos generan mucho calor y utilizan electricidad. Querrá mantener sus costos de electricidad a $ 0.13 kwh o menos. Si tiene paneles solares instalados en su hogar, entonces podría proporcionarle un incentivo adicional para que se someta a este tipo de operación, ya que también está produciendo electricidad. La computación en la nube junto con la productividad de energía renovable puede permitirle vivir de los activos. La minería de criptomonedas es una empresa comercial de volumen y no tan inmediata como rentable. Cuando se resume, se cree que el punto de equilibrio típico para esta empresa sabrosa que incluye hardware, internet y costo de la electricidad oscila entre 18 y 24 meses en promedio. Aunque, algunos mineros de criptomonedas menos invertidos han calculado alcanzar su punto de equilibrio después de 4 años.

La necesidad de una tarjeta gráfica de alta calidad proporciona una ventaja para los jugadores con PC de juegos para ejecutar un software similar, pero aún puede ser necesario configurar dispositivos de hardware externos adicionales para ejecutar la operación. Sin embargo, hay oportunidades que se ofrecen en los juegos de PC que te permiten extraer mientras estás lejos de tu computadora e incluso Pokemon Go ha integrado Bitcoin en su sistema de recompensas, así como juegos en la tienda Google Play y App Store que te recompensan con criptomonedas. Sin embargo, la mayoría de los juegos se ejecutan con ingresos publicitarios, que es la forma en que pueden pagarle solo por jugar un juego. Tan pronto como alcance el umbral mínimo, podrá transferir los fondos a su billetera virtual. Finalmente, el navegador Crypto Tab es otra herramienta que le permite extraer Bitcoin mientras navega en línea y visita sitios web y otro contenido. Según los informes, las ganancias son bajas, a menos que pueda crear un grupo de minería y compartir el navegador con su red, entonces puede multiplicar sus ganancias.

Crypto TAB Browser retiro de efectivo mínimo 0.00001 BTC o $ 0.08 Agregar amigos a su red le permite minar con amigos y ganar más dinero.

El Navegador Crypto https://get.cryptobrowser.site/10386657

Gastamos mucho dinero en nuestras máquinas y dispositivos, ¿por qué no ganar dinero con los equipos de capital que albergamos en nuestros hogares? En última instancia, las recompensas de devolución de efectivo en su tarjeta bancaria y los reembolsos ofrecen a los usuarios un incentivo para comerciar y comprar, pero solo es tan bueno como la cantidad que uno gasta. Hoy en día, incluso hay tarjetas bancarias diseñadas con criptomonedas que le devuelven el 1% de los dólares que gasta en la tarjeta en Bitcoin.

Gana mientras juegas

Hoy hay una nueva ola de entretenimiento que se gana mientras juegas. Pocos millennials pueden recordar un momento en que fueron a una sala de juegos para jugar un juego y gastaron unos pocos dólares en una máquina. Incluso menos jugadores podrían recordar el costo de jugar Pac-Man, simuladores de arcade de carreras o videojuegos de First Person Shooter y pagar $ 0.50 o menos. Hoy en día, los jugadores móviles pueden gastar cientos o incluso miles de dólares jugando una aplicación de juegos. Tradicionalmente, los juegos se jugaban en salas de juego, se alquilaban o compraban para una consola de videojuegos estacionaria que se usaba en casa. Los tiempos están cambiando y hay una tendencia en curso con las compañías de juegos que están pagando al público para descargar y jugar sus juegos. Sin embargo, no todo aquí es lo que parece. Probablemente ya haya visto anuncios de estas aplicaciones que afirman que puede ganar dinero con ellas. Por supuesto, estas cifras son exageradas y puede que no valgan la pena para algunos, dado que la cantidad de dinero que puede

ganar con estas aplicaciones es de unos pocos centavos por semana. Es posible que vea a las personas en estos anuncios con una cantidad sustancial de dólares en sus manos alegando que obtuvieron todo ese dinero solo por jugar. No es tan afortunado, la realidad es que los jugadores están ganando tokens que pueden intercambiarse por tarjetas de regalo: PayPal, Amazon y en otras tiendas una vez que alcanzan el umbral mínimo, normalmente $ 10. Lo que hacen estas aplicaciones es pagar a los usuarios una fracción de sus ingresos publicitarios, es decir, el dinero que ganan cada vez que los usuarios ven videos, responden encuestas y compran productos o servicios de los enlaces de afiliados.

El hecho de que estas compañías se presenten como una forma de que las personas ganen cantidades obscenas de dinero jugando sus juegos es una burla. El algoritmo se controla para pagar hasta después de que hayan obtenido ganancias significativas de usted. Entonces, si logra cobrar esos $ 10 eventualmente, simplemente piense que probablemente ganaron $ 100 o más mostrándole innumerables videos, lo que le permite responder preguntas de la encuesta que después de responder unas 10-20 preguntas y una vez que obtiene ciertos datos e información de marketing, puede ser descalificado y perder la recompensa. En la actualidad, el contenido se valora y los datos son el rey. De hecho, los datos son tan importantes que las compañías pueden incluso usar sus datos para vender a otras compañías como clientes potenciales. Esta acción afecta la privacidad del usuario. El escándalo más reciente entre Facebook y Cambridge Analytica en 2018 mostró cómo los datos de los usuarios se pueden usar como producto o ventas potenciales para vender a otra compañía y pueden servir como un flujo constante de ingresos para los desarrolladores web y de aplicaciones por igual. En estas aplicaciones puede haber una larga lista de ofertas o tareas que hacer para ganar monedas y las recompensas pueden depender del tamaño de la tarea o la oferta. Por ejemplo, una oferta puede ser descargar otra aplicación de juegos y alcanzar el nivel 15 con una recompensa de 1,000,000 de monedas que puede ser el equivalente a $ 50. Excepto que quizás no se dé cuenta de que el juego que acaba de descargar está diseñado para que los usuarios compren gemas, recursos y otras actualizaciones. Para obtener más información sobre este tema de los juegos, consulte el libro 1. Otra forma de ganar a través de estas aplicaciones es si acepta comprar un producto o servicio en la aplicación. Puede ser una suscripción VPN, un software de limpieza de la nube, Fender Play, otra aplicación de juegos o un servicio telefónico, etc. En resumen, obtienes una ligera recompensa en la aplicación que puedes canjear por dólares. Evidentemente, es posible que no obtenga los mismos beneficios para su cuenta al ver los anuncios que obtendría al completar una oferta formal. Cuando miras anuncios y compras un anuncio de video, la única recompensa que obtendrás es otro turno en el juego, incluso si pagas por algo. Y en caso de que no lo supieras en este momento, el dinero es energía. Si alguna vez ha ejecutado una campaña publicitaria, comprenderá por el hilo que acabamos de cubrir cómo se gasta su dinero. Hay una larga lista de YouTubers que ganan dinero publicando anuncios en sus videos. Las aplicaciones y YouTubers con una audiencia de 100,000 suscriptores y descargas pueden ejecutar exitosamente anuncios en sus videos y recibir pagos por ello. Al anunciar o promocionar un producto, todo el dinero que decide inculcar

en su campaña publicitaria se acumula y se distribuye a través de Internet a través de una serie de canales de distribución y el dinero se distribuye en una gran cantidad de cuentas de espectadores. En pocas palabras, al público objetivo se le paga por un momento de su capacidad de atención. Puede ser un anuncio de texto o video utilizado para atraer a los espectadores. En la siguiente sección, veremos algunas de las herramientas que puede usar para ejecutar estos anuncios y cómo analizarlos.

Herramientas para publicidad en línea

Si está tratando de aumentar el tamaño de su audiencia, es posible que desee ejecutar una campaña publicitaria. Hay dos herramientas que me gustaría discutir en este capítulo para explicar cómo ejecutar una campaña publicitaria y recopilar datos de ella. Ahora que sabe cómo se gastará su dinero en la campaña, en cualquier serie dada de combinaciones, el dinero representa la energía que se puede traducir a créditos y, de cualquier manera, es prácticamente agarrada por cualquiera, aunque sea involuntariamente, así como aquellos quienes eligen capitalizar la situación y ganar dinero por ser un miembro EXTRA de la audiencia. De cualquier manera, se paga dinero a aquellos que pueden conducir y (en un sentido maquiavélico) vender influencia; promoviendo así productos y / o servicios en la web. En primer lugar, considere el tipo de anuncio que le gustaría publicar. Es crucial publicar anuncios para promocionar su empresa y obtener clientes. Es por esa razón, que hoy, el consumidor está más iluminado de lo que era en el siglo anterior. De hecho, el concepto del consumidor educado no surgió hasta la década de 1980. Además, Internet es mucho más eficiente que los anuncios impresos en la actualidad; ya que las masas tienden a conectarse a internet a través de nuestros dispositivos en busca de información. La evidencia muestra que, en general, nuestras necesidades de interactuar con Internet de las cosas (IoT) y usar esos dispositivos de teléfonos inteligentes (a menudo colocamos un pedestal) también reemplaza la antipatía de la mayoría hacia la lectura de periódicos impresos y otros materiales impresos . En el siglo XV, la imprenta Guttenberg en el sur de Alemania incitó una revolución mundial que hizo que la gente aprendiera a leer. La información se promulgó a través de material de papel impreso, y la cantidad de personas que aprendieron a leer aumentó exponencialmente. Más de 500 años después, y las masas están utilizando sus dispositivos digitales para leer información, y lo que es más importante, la comunicación instantánea remota ha sido un factor fundamental en ese sentido.

Sin duda, la publicidad en papel está en declive y el marketing digital está creciendo. En cualquier caso, el arte de comunicarse con los consumidores ha existido desde el inicio de la sociedad civilizada y el consentimiento del contrato social. Las empresas utilizan muchas tácticas para adquirir más clientes. No importa si las estrategias utilizadas por las empresas hoy en día se implementan en el mundo real, como en la calle, en cuadras de la ciudad o mediante escrutinio, puerta a puerta, vallas publicitarias y / o a través de un medio digital. Mientras la información llegue al consumidor, se logra el objetivo. Sin embargo, la publicidad en línea es quizás el método más efectivo hasta la fecha para permitir que su empresa esté ampliamente expuesta a

la mayor cantidad de personas a la vez y en todas las regiones geográficas. El conocimiento es poder, dijo Albert Einstein. Así que aquí, sin hacer nada más, profundizaremos en cómo ejecutar un anuncio en todo el mundo y aprender a analizar los datos de nuestros espectadores y / o visitantes.

Anuncios Google

Para comenzar, Google Adwords es una plataforma de publicidad de pago por clic que le permite comprar exposición en la web a través de anuncios de texto y videos con una duración mínima de tiempo de visualización entre 15-30 segundos. Google AdWords le ofrece publicidad de pago por clic, lo que significa que solo paga por los resultados. De hecho, ejecutar una campaña en Google AdWords le permite dirigirse a audiencias específicas y rastrear ubicaciones geográficas específicas. El costo por clic de la publicidad puede ser de $ 0.01 a $ 0.10, esto puede variar de vez en cuando y significa que por cada persona a la que llegue durante la promoción de su marca, tendrá que pagar unos centavos de cada dólar. tu campaña Puede configurar fácilmente una categoría o tema adjunto a su anuncio, y activar o desactivar el anuncio o pausar instantáneamente su campaña en cualquier momento del día. Se le facturará después del primer mes o hasta que alcance su límite. Para una campaña de Google AdWords que cueste entre $ 10 y $ 20, puede hacer que una pequeña campaña se ejecute de manera constante durante no más de un par de semanas y obtenga 141-235 clics por día. La optimización de motores de búsqueda SEO es una parte integral de ser reconocible en Internet. Si desea que su negocio se encuentre en la web y quiere ser transparente para adquirir más suscriptores, Google Adwords es una plataforma importante para su negocio porque lo lleva a la cima de las listas de búsqueda en su motor de búsqueda. Google posee una gran base de datos de información y es quizás la compañía de Internet más poderosa hasta la fecha. Sin embargo, cualquiera puede crear un sitio web malicioso y usar Google AdWords para impulsar su aparición en los resultados de los motores de búsqueda y en los escritorios de las víctimas desprevenidas. En pocas palabras, los delincuentes también hacen promociones. Es inaceptable mentir a los clientes. Hay un tabú con hacer clic en los listados de búsqueda promocionados porque generalmente tienen la menor relevancia y están orientados a obtener algo del usuario en lugar de satisfacer sus necesidades reales. Aunque, Google se somete a controles específicos para aprobar el anuncio (que lo dirige a la página de destino), el anuncio aún puede ser un impostor. Las funciones consecutivas en el sitio web pueden llevar a un usuario a una página de destino diferente en el sitio web y solicitar que el usuario ingrese su información de inicio de sesión para robarles datos.

Google Analitica

La próxima plataforma que discutiremos se usa para analizar datos e informar el historial de tráfico web a su sitio. Es importante conocer la fuente de su audiencia. Si está construyendo una marca o está en una misión en la web haciendo un trabajo de reconocimiento para localizar a un enemigo; no obstante, obtener esta información de marketing inherente le permite obtener información. Google Analytics se puede utilizar para proporcionar información relacionada con el tráfico web, como la duración de la sesión, las páginas por sesión, la tasa de rebote y más. Puede rastrear la ubicación geográfica de un usuario y descubrir la demografía del mercado. Google Analytics se puede bloquear a través de extensiones de navegador web y firewalls. El servicio es de uso gratuito con cualquier cuenta de Google. Para que Google Analytics funcione, debe instalar un código de seguimiento único en cada página de su sitio web. El código de seguimiento es un pequeño fragmento de lenguaje de codificación Javascript que se ejecutará en el navegador y registrará información sobre los visitantes. Los piratas informáticos pueden manipular esta herramienta con bastante facilidad utilizando su ID de propiedad en una página web diferente y eso dificultará el acceso a su página. Como ya hemos dicho, hay un código de seguimiento único incrustado en cada página. Para acceder al código, deberá hacer clic derecho en una página web y hacer clic en Ver fuente de la página. Luego verá un código largo escrito dentro de la ventana del navegador en lugar de la página web. Para obtener el ID de propiedad, presione control + F o comando + F y busque "ga.js", entonces tendrá la información para ingresar a otra página web. En efecto, esta acción puede dañar los datos del sitio web y, si se realiza correctamente, puede enviar los datos a cualquier cuenta de Google.

Vulnerabilidad de Wi-Fi

Para aquellos usuarios de teléfonos inteligentes con Wi-Fi público gratuito, una vez integrados en la red, su seguridad puede ser vulnerable a los ataques cibernéticos. De hecho, el uso de una conexión Wi-Fi pública gratuita en una escuela, empresa u otro tipo de lugar público es la razón principal por la que decido usar una VPN que permita encriptar la actividad del usuario en el dispositivo, agregando así una capa adicional de privacidad para todos nosotros. En esta sección, analizaremos una vulnerabilidad importante de los activos de protección de Wi-Fi (WPA2) y los problemas que surgieron cuando los piratas informáticos descifraron las redes encriptadas. Existen claves de cifrado únicas para cada cliente inalámbrico proporcionadas por la red WPA2 que se conecta a la red Wi-Fi. Según el producto de Internet de las cosas (IoT), cualquier dispositivo inteligente (que se conecta a Wi-Fi), como reloj inteligente, teléfono inteligente, TV, computadora portátil, dispositivos portátiles y dispositivos, cada dispositivo tiene, por así decirlo, una clave de cifrado única y también se puede poner en riesgo de ataques cibernéticos. Cuando esto sucede, esto puede distorsionar la funcionalidad del dispositivo. Entre otros inconvenientes de Wi-Fi, el ancho de banda de la LAN inalámbrica está muy limitado a un cierto número de dispositivos. Las conexiones

a Internet 5G le permiten conectar hasta 100 dispositivos a su red, sin embargo, cuando se encuentra en un Wi-Fi público gratuito, la conexión puede retrasarse tan pronto como se haya alcanzado el ancho de banda máximo. En cualquier caso, los piratas informáticos pueden conectarse con usted de igual a igual a través de la misma red.

Hay muchos dispositivos, sin importar el sistema operativo utilizado macOs, iOs, Windows, Linux y Android, todos ellos pueden verse afectados por las vulnerabilidades de Wi-Fi, eso es porque una vez que los clientes están prácticamente conectados a la red, están expuestos de la misma manera . Una red Wi-Fi abierta puede permitir que un atacante descifre el tráfico de Wi-Fi en otros dispositivos en la misma red, lo que significa que puede conocer el historial de navegación del dispositivo de otro usuario; también realice la inyección de contenido e inserte ataques de spam o phishing, o intercepte el punto final de las comunicaciones: conexiones TCP (tomas de Internet). Entraremos en PenTesting en el próximo capítulo y cubriremos algunos aspectos del pirateo ético. En términos generales, dado que las personas en la misma red quieren poder obtener una cantidad igual de acceso a Internet, puede haber dificultades cuando hay una cantidad limitada de ancho de banda disponible. Desafortunadamente, cuando hay un ancho de banda limitado disponible, esto puede desencadenar ataques de denegación de servicio que pueden interrumpir el acceso a un sitio web. La cantidad de tiempo que tomaría liberar el ancho de banda dependería de la actividad y la presencia de las personas que están allí junto con usted usando el Wi-Fi público. Puede que tenga que actualizar un cierto número de veces. Además, la aparente debilidad está en el llamado apretón de manos de cuatro vías del protocolo WPA2. Este es un proceso de cuatro pasos que valida las credenciales de un usuario de la red. Es esencialmente un intercambio que garantiza que el usuario conozca la contraseña de la red.

Una vez allí, un hacker puede acceder a través de un punto de entrada aceptado. Para proteger mejor su dispositivo, debe cerrar todas las puertas traseras. Descargue actualizaciones de software para su dispositivo tan pronto como estén disponibles. Estas actualizaciones surgen generalmente una vez que el ingeniero / desarrollador de software ha solucionado ciertos errores / problemas con la versión anterior. Solo piense que no querría mantener la puerta principal y las ventanas abiertas mientras duerme y / o está lejos de casa. Cambiar la contraseña o el enrutador de la red Wi-Fi no solucionará el problema ni le ayudará en futuras amenazas cibernéticas. Los ataques de Krack aún pueden infiltrarse en la mayoría de los dispositivos habilitados para Wi-Fi. Para suavizar el daño, debe evitar ingresar datos confidenciales en sitios que usan cifrado https. Finalmente, debe obtener una VPN para mantenerse protegido en redes Wi-Fi aleatorias.

Pen Testing

Es importante tener en cuenta que muchas personas hoy en día se involucran en Pen Testing por todas las razones equivocadas. En primer lugar, cuando hablamos del término "Pen Testing" denota una práctica de piratería ética. Los buenos intentan entrar en la red de su sistema para tratar de encontrar formas en que un hacker malicioso

pueda robarle datos. Si se encuentra una debilidad, se hacen recomendaciones de seguridad. Los Pen Testers pueden encontrar agujeros en su red y atacar de la misma manera que lo hace un hacker. Dado que hay muchas formas de explotar las vulnerabilidades del sistema según el nivel de seguridad y cómo hacer Pen Testing en la nube, es mejor consultar con un experto. El valor de Pen Testing es incalculable, ya que se puede utilizar para lograr fines buenos y malos. Sin embargo, si bien los piratas informáticos de sombrero blanco y los piratas informáticos de sombrero negro tienen la capacidad de realizar Pen Testing, deja de ser una "prueba" cuando los piratas informáticos acceden a sus datos para beneficio personal. El objetivo principal de Pen Testing es practicar la prueba de ingresar a un sistema informático, red o aplicación web e identificar debilidades de seguridad explotables. Hay un elemento de confianza entre usted y el hacker ético. Las empresas pueden usar Pen Testing para obtener la opinión de un tercero experto, cumplir con ciertas leyes y regulaciones, así como también para investigar y detectar su nivel de defensa cibernética.

Existen tres tipos de modelos de computación en la nube que se pueden usar para implementar recursos. En primer lugar, Infraestructura como servicio o (IaaS) que atribuye a la infraestructura de computación en la nube, y también incluye servidores, redes, sistemas operativos y almacenamiento que se proporciona a una empresa u organización a través de un tablero o API (interfaz de programación de aplicaciones) y les ofrece control sobre sus servidores y almacenamiento en el centro de datos. Entre las ventajas están que la compra del hardware está correlacionada con el consumo de datos. Por lo tanto, se dice que IaaS es el modelo de computación en la nube más flexible. Pagas por lo que usas. Por otro lado, existe un problema de seguridad con respecto a IaaS ya que la comunicación de datos puede estar expuesta desde el host a otras máquinas virtuales (VM). Ver VirtualBox et al. En segundo lugar, queremos ver Plataforma como servicio o (PaaS), el proveedor entrega herramientas de hardware y software al cliente para ejecutar una aplicación a través de Internet. Muchos proveedores públicos de PaaS pueden prohibir la prueba de la pluma porque interrumpirá el servicio y también pondrá en riesgo a los clientes de la compañía. PaaS se puede entregar a través de servicios en la nube públicos, privados e híbridos, como el alojamiento de aplicaciones y el desarrollo de Java. Los usuarios tienen la ventaja de acceder a la plataforma desde un navegador web en cualquier computadora. El tercer modelo de computación en la nube Software as a Service (SaaS) en el que una empresa proporciona un software de aplicación en la nube, actualizaciones automáticas por suscripción para los clientes. Las compañías SaaS pueden contratar trabajadores independientes con el conocimiento y la experiencia necesarios en lugar de los ingenieros de software habituales.

Empresas de computación en la nube

Infraestructura como servicio **IaaS** Amazon Web Services (AWS), Rackspace

Plataforma como servicio **PaaS** Microsoft Azure, Cloud Bees

Software como servicio **SaaS** SalesForce.com, Verizon, Mailchimp.com

A continuación, me gustaría discutir un ejemplo del mundo real que nos brindan algunos expertos sobre cómo los Pen Testers pueden infiltrarse en una empresa. En cualquier caso, hay un poco de engaño involucrado. La mayor parte del trabajo de reconocimiento implica obtener información del perfil de la empresa y saber cómo está estructurada. ¿Cuáles son sus sistemas? ¿Cómo se enmarcan sus direcciones de correo electrónico? Se requiere planificación estratégica para lograr los objetivos. Para hacer Pen Testing, un hacker ético tendrá que obtener acceso a la red y / o hardware. En una historia sobre un Pen Tester que fue contratado para exponer las vulnerabilidades de una empresa, pudo infiltrarse en el banco fingiendo ser un repartidor de pizzas. Supuestamente estaba allí para vender pizza a los empleados por porción. Incluso compró el sombrero, la camisa y todo el atuendo para interpretar el papel. Había desarrollado todo este esquema en línea donde aprendía los correos electrónicos de todo el personal, pero necesitaba recibir el correo electrónico de la recepcionista, que era realmente el único que podía permitirle ingresar a las instalaciones. Una vez que llegó, tenía todos los correos electrónicos listos para ser enviados y logró aprender el nombre y el apellido de la recepcionista de su etiqueta de nombre, y con eso, pudo enviar los correos electrónicos a todo el personal. Creó cuentas de correo electrónico falsas similares a las de los jefes y en la incertidumbre inminente) mientras la recepcionista intentaba confirmar el evento,) pidió ir al baño que estaba detrás de puertas cerradas; luego, pudo ingresar a la instalación sin supervisión mientras la recepcionista revisaba para verificar las fuentes. En resumen, en el tiempo que le llevó comprobar que ya había recorrido el edificio y regresado. Había completado su misión. Al final, el Pen Tester que eligió permanecer en el anonimato utilizó el arte del engaño para obtener acceso a las instalaciones y, al mismo tiempo, pudo comprometer algunas estaciones de trabajo donde enchufó un conjunto de dispositivos externos.) que instalarían aplicaciones de software malicioso en los sistemas operativos.

Conclusión

Todo lo que está conectado a Internet posee un medio de comunicación inalámbrico que tiene ventajas y desventajas. Sin lugar a dudas, muchas cosas están sucediendo hoy

en día en el mundo de la ciberseguridad y el consumidor educado está cada vez más consciente de estos problemas. Al hacer clic en los enlaces, visitar ciertos sitios web nos pone en riesgo de ser blanco de estafas y robos. Gran parte de la industria de Internet y comercio electrónico está controlada por los ingresos publicitarios y cada usuario en la web está dirigido a los consumidores. Con tan gran poder y responsabilidad, hay forma de usar herramientas para agregar a su privacidad en línea. En este libro, hemos cubierto plataformas que pueden permitirle usar estrategias defensivas y ofensivas al navegar en la web desde su dispositivo. Hemos hablado sobre cómo disfrazar enlaces y cómo rastrear clics en esas mismas URL. Encontrar la ubicación de un usuario es una parte integral del reconocimiento de edificios. Una red privada virtual le permite navegar por la web de forma privada. Al mismo tiempo, ejecutar una máquina virtual en su dispositivo, como Virtual Box, también agrega una capa adicional de seguridad a sus dispositivos. Una computadora dentro de una computadora. Además, hemos identificado las llamadas automáticas y las estafas en línea como problemas principales relacionados con la actividad fraudulenta en la web. El mercado de criptomonedas es una red compatible entre pares. Los bitcoins, entre otras monedas, permiten un medio de intercambio descentralizado. Sin duda, la volatilidad de los precios ya que el precio de un Bitcoin ha demostrado variar cuando cada rango de varios miles de dólares en precio podría proporcionar una diferencia sustancial para el titular de la cuenta al cobrar. Sin embargo, siempre he tenido la percepción de que las criptomonedas demostrarían ser un activo en la exploración espacial, ya que compañías como la NASA, Amazon y Space-X se esfuerzan por colonizar Marte. Finalmente, se esperaba que para el año 2030 pudiéramos aterrizar el primer equipo de seres humanos en el planeta Marte. En otras palabras, creo que las criptomonedas podrían usarse como un medio de intercambio utilizado en diferentes planetas. Algo así como una moneda interestelar, Bitcoin, Ethereum, Litecoin, etc. podrían usarse en el espacio para ser intercambiados entre la sociedad civilizada en caso de aterrizar y establecerse en la Luna y / o Mars et al.

Hay muchas formas de ganar dinero en Internet. Internet es tu ostra. El ingreso pasivo es quizás el mejor tipo de ingreso ya que solo tiene que hacer el trabajo una vez. Es posible que desee crear anuncios relacionados con su marca o producto. Con suerte, algunas de las plataformas y herramientas utilizadas para analizar la demografía resultarán útiles en sus futuros emprendimientos. Google Adwords y Google Analytics son dos plataformas compatibles con el popular motor de búsqueda que pueden ayudarlo en su campaña desde la publicación de su anuncio hasta la creación de investigación de productos y generar estadísticas de audiencia e información sobre la demografía existente. Por cada interés que tenga, hay una plataforma de redes sociales que lo respalda. ¿Puede mantener familiares y amigos cercanos en la misma red? Recomienda Facebook ¿Eres interesante en política y puedes expresarte con palabras concisas? Recomienda Twitter ¿Puedes compartir fotos y videos que generen una gran cantidad de interés? Instagram y YouTube. ¿Tienes tu propio sitio web y dominio? ¿Escribes un blog? Si no, podría estar ganando dinero todos los meses. ¿Quieres que te paguen por hacer preguntas? Usa Quora. Cuando está conectado a una gran cantidad de usuarios en cualquier plataforma de redes sociales, puede garantizar la maximización de sus

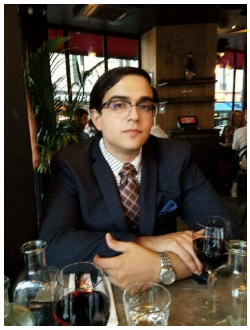
ganancias. Al tratar con Internet en las últimas dos décadas, hemos visto la proliferación del intercambio de archivos, el intercambio económico y hemos sido testigos de muchas actividades web oscuras utilizadas para infiltrar empresas y proteger servidores de bases de datos.

Internet es un canal monetario. El lado oscuro de Internet contiene métodos utilizados para mantener la privacidad, pero al mismo tiempo estas fuerzas pueden participar en actividades fraudulentas. La preocupación con respecto a Bitcoin como un instrumento para el lavado de dinero no es decir que el lavado de dinero no ocurre mediante el uso de dinero en efectivo. Después de todo, han pasado más de 100 años desde que la mafia se extendió en las grandes ciudades para participar en actividades ilícitas y canalizar su dinero sucio a través de diferentes actores y / o cuentas bancarias extraterritoriales. En otras palabras, no hay evidencia suficiente para respaldar que la cantidad de lavado de dinero que usa Bitcoins excede o es igual a la cantidad de lavado de dinero impulsado por dólares. Los resultados son iguales. Sin embargo, el problema real con las billeteras virtuales y las criptomonedas es que la Policía y el FBI no pueden acceder a redes y cuentas encriptadas. Esto es lo que perturba a la mayoría de las autoridades, ya que la propiedad incautada sigue siendo prácticamente inaccesible. La cantidad de anuncios a los que las personas están expuestas en un día determinado excede la cantidad de publicidad que una persona había visto en ese momento en la década de 1970. En retrospectiva, estuvimos expuestos a aproximadamente 500 anuncios por día, mientras que hoy se estima que los seres humanos están expuestos a al menos 5,000 anuncios por día. Además, los expertos en marketing digital estiman que la mayoría de los estadounidenses pueden estar expuestos a alrededor de 4,000 a 10,000 anuncios por día. La industria del entretenimiento está creciendo enormemente. La gente está jugando aplicaciones de juegos por dinero en efectivo. Estas aplicaciones móviles son compatibles con anuncios que incluyen videos diseñados para atraer a los compradores. La proporción del tiempo para recompensar es bastante exhaustiva y la gente podría jugar este juego durante horas sin cobrar. De hecho, el camino para cobrar premios en efectivo a través de aplicaciones de juegos está lejos de ser dinero rápido, especialmente por dinero en grandes cantidades.

Glosario

Ataque de denegación de servicio (DDOS) Un ataque DDOS es un ataque cibernético que hace que una máquina o recurso de red no esté disponible para sus usuarios previstos a través de una sobrecarga de tráfico.
Almacenamiento en frio El almacenamiento en frío es una billetera fuera de línea donde puede almacenar criptomonedas.
Bitcoin es la criptomoneda original. Es una moneda descentralizada y sirve como la forma más común de comprar información, productos y servicios en la web oscura.
Bitcoin Cash Es un spin off de la criptomoneda de Bitcoin.
Botnet Una botnet es un grupo de dispositivos conectados a Internet controlados y diseñados para realizar diversas tareas. Por lo general, están infectados con malware y controlados sin el permiso de su propietario.
Cardadura Cardar es la práctica de vender y robar información de tarjetas de crédito.
Clearnet Clearnet se refiere a sitios web que pueden ser visitados por cualquier navegador sin el uso de servidores proxy. Por lo general, estos son sitios web que son rastreados por los motores de búsqueda y se pueden encontrar a través de la búsqueda.
Criptomoneda La criptomoneda es una moneda digital que se puede usar de forma anónima.
Dark Web el Dark Web es la porción de la red oscura que contiene actividades ilegales o inmorales.
Dox Dox es el acto de revelar la verdadera identidad de una persona anónima.
Dumps es una publicación pública masiva de datos.
Litecoins Las litecoins son una criptomoneda basada en un protocolo de código abierto.
Malware El malware es un software malicioso que se utiliza para interrumpir las operaciones de una computadora o dispositivo móvil, obtener información confidencial, acceder a un sistema informático privado o exhibir publicidad no deseada.
Mercado Un mercado es un sitio web donde un usuario puede comprar bienes o servicios.
Monero Monero es una criptomoneda de código abierto.
RAT Herramienta de administración remota
Un RAT es un software que permite a sus usuarios controlar otro dispositivo a distancia con la misma facilidad de uso que tendrían con acceso físico a la computadora.
Red oscura La red oscura incluye cualquier parte de Internet que no esté indexada por los motores de búsqueda y solo se puede acceder a través de un software especializado.
Red profunda Similar a la red oscura, la web profunda es la parte de Internet que no está indexada por los motores de búsqueda y solo se puede acceder mediante software especializado.
Suplantación de identidad El phishing ocurre cuando alguien envía fraudulentamente un correo electrónico supuestamente de una fuente confiable para obtener credenciales o información.
Red privada virtual (VPN) Una red privada virtual (VPN) es una pequeña red de computadoras que se conectan a una red pública, como Internet. Existen muchos usos legítimos para las VPN, como permitir que los empleados de una empresa se conecten a

una LAN privada de forma remota o aumentar la seguridad. Pero las personas en la web oscura usan VPN para enmascarar su dirección IP. Esto hace que sea más difícil para cualquier persona rastrear su ubicación si usa la web oscura para hacer algo ilegal.



El Lado Oscuro de Internet: Descubriendo Datos y Privacidad
Sobre el autor: Telly Frias, Jr.

Emprendedor digital. Ventas y marketing. Logística de almacén y cadena de suministro. Tecnologías de la información. Máster en Administración de Empresas y Marketing. Bachiller en Ciencias Políticas y Grado Asociado en Lenguas Modernas.

También asegúrese de ver la primera parte de esta serie
Cibercrimen: Las Amenazas al Navegar en Internet y las Redes Sociales.