Algunas consideraciones para la ciberseguridad en el Streaming:

a. Definición y funcionamiento del streaming: El streaming es una tecnología que permite compartir y enviar contenido multimedia en tiempo real a través de servidores, sin necesidad de descargarlo [1]. Puede ser en vivo o grabado, y muchas plataformas cargan automáticamente el contenido después de la transmisión.

b. Popularidad del streaming: En la actualidad, el streaming ocupa una gran parte del mundo virtual y se ha convertido en algo habitual en nuestras vidas como usuarios.

c. Tendencias y rankings en el streaming: Es importante conocer qué tipos de contenido son los más consumidos a través del streaming, como películas/series, música, gaming/esports/IRL, videos on demand, podcast/webcast.

Ciberseguridad:

a. Riesgos de ciberseguridad en el streaming: Es fundamental comprender los posibles riesgos asociados con el streaming en línea, como malware, estafas de phishing y piratería informática, que pueden comprometer la seguridad de la información personal y financiera.

b. Privacidad y seguridad en el streaming: Se deben tomar ciertos recaudos al disfrutar de plataformas de streaming, como configurar correctamente los datos de las cuentas y corroborar la legitimidad de cada aplicación.

c. Ciberseguridad para influencers: Los influencers deben tomar en serio la seguridad de sus datos para proteger su credibilidad y la confianza de su audiencia. Es recomendable verificar la integridad de las cuentas y considerar la inversión en legitimidad o verificación.

d. Comunicación en caso de ataques: En caso de ser víctima de un ciberataque, es importante comunicarlo a otros influencers de confianza para contener el impacto y proteger a la audiencia.

Influencers:

a. Importancia de la seguridad para los influencers: Los influencers y personajes públicos han sido víctimas de varios tipos de ataques informáticos, lo que compromete su credibilidad y la confianza de su audiencia. La seguridad de los datos es crucial para proteger la imagen y la privacidad .

b. Verificación de integridad de la cuenta: Se recomienda verificar que la cuenta no haya sido comprometida y utilizar plataformas que permitan la verificación de la identidad .

Riesgos de ciberseguridad en el streaming en línea: Es importante comprender los posibles riesgos asociados con el streaming en línea, como el malware, las estafas de phishing y los intentos de piratería informática, que pueden comprometer la seguridad de la información personal y financiera de los usuarios.

Aumento del uso de servicios de streaming durante la pandemia: La pandemia de COVID-19 ha llevado a un aumento significativo en el uso de servicios de streaming, ya que las personas buscaban contenido continuo para mantenerse entretenidas durante los períodos de confinamiento .

Definición y funcionamiento del streaming: Es importante comprender qué es el streaming y cómo funciona. El streaming permite compartir y enviar contenido multimedia en tiempo real a través de servidores, sin necesidad de descargarlos. Puede ser en vivo o grabado, y muchas plataformas cargan automáticamente el contenido después de la transmisión.

Servicios de streaming legales y seguros: Se recomienda utilizar servicios de streaming legales y confiables, como Amazon Prime, Netflix y NOW TV, ya que estos suelen implementar medidas de seguridad reforzadas para proteger los datos de los suscriptores .

Mantenerse actualizado sobre tendencias y riesgos: Es importante mantenerse informado sobre las últimas tendencias en el mundo del streaming y la ciberseguridad. Mantener contacto con expertos en ciberseguridad puede proporcionar asesoramiento valioso y asegurarse de que la información compartida sea precisa y orientada correctamente .

Considerar riesgos específicos en el streaming en vivo: En el caso de transmisiones en vivo, es esencial recordar que no hay filtros ni ediciones al contenido que se transmite en tiempo real, lo que puede generar situaciones impredecibles y potenciales riesgos. Se debe tener en cuenta la importancia de la conciencia de los riesgos y la protección de los sistemas.

Al recopilar y organizar esta información, podrás proporcionar un sólido respaldo académico para tu conferencia sobre streaming y ciberseguridad. Recuerda citar las fuentes relevantes durante tu presentación para respaldar tus puntos con evidencia sólida.

Sección 1: Ciberseguridad

1.1 Riesgos de Ciberseguridad

Los ciberdelincuentes pueden intentar acceder a tus datos personales y financieros a través de ataques informáticos.

Los mensajes y ofertas tentadoras pueden contener archivos o software maliciosos.

1.2 Privacidad y Seguridad en el Streaming

Configura correctamente tus datos en las cuentas de streaming para proteger tu privacidad.

Verifica la legitimidad de las aplicaciones antes de utilizarlas.

1.3 Ciberseguridad para Influencers

Importancia de proteger la seguridad de los datos para mantener la credibilidad y confianza de la audiencia.

Verifica la integridad de tus cuentas y considera invertir en legitimidad o verificación.

1.4 Comunicación en Caso de Ataques

Comunica cualquier ciberataque a otros influencers de confianza para contener el impacto y proteger a tu audiencia.

Sección 2: Streaming

2.1 Definición y Funcionamiento del Streaming

El streaming permite compartir y enviar contenido multimedia en tiempo real sin necesidad de descargarlo.

Las plataformas de streaming cargan automáticamente el contenido después de la transmisión.

2.2 Tendencias y Rankings en el Streaming

Conoce los tipos de contenido más consumidos a través del streaming, como películas/series, música, gaming/esports/IRL, videos on demand, podcast/webcast.

Sección 3: Influencers

3.1 Importancia de la Seguridad para los Influencers

Los influencers y personajes públicos han sido víctimas de ataques informáticos que comprometen su credibilidad y la confianza de su audiencia.

3.2 Verificación de Integridad de la Cuenta

Verifica que tu cuenta no haya sido comprometida y utiliza plataformas que permitan la verificación de identidad.

En este documento, encontrarás información valiosa y consejos prácticos para proteger tu privacidad y seguridad en línea, así como aprovechar al máximo el mundo del streaming y convertirte en un influencer exitoso.

Sección 1: Ciberseguridad

La ciberseguridad es una preocupación creciente en nuestro mundo digital. Para proteger tus datos personales y evitar ser víctima de ataques informáticos, es importante seguir estas pautas:

Riesgos de Ciberseguridad: Los ciberdelincuentes están al acecho. Asegúrate de desconfiar de mensajes y ofertas sospechosas, ya que podrían contener archivos o software maliciosos. Mantén tus dispositivos protegidos con contraseñas seguras y actualizaciones regulares.

Privacidad y Seguridad en el Streaming: Al disfrutar del streaming, ten en cuenta los siguientes aspectos . Configura adecuadamente tus cuentas de streaming para proteger tu información personal. Verifica la legitimidad de las aplicaciones que utilizas y evita proporcionar datos innecesarios.

Ciberseguridad para Influencers: Si eres un influencer o aspiras a serlo, debes prestar especial atención a la seguridad de tus datos . Verifica regularmente la integridad de tus cuentas y considera invertir en legitimidad y verificación. Además, mantén una comunicación abierta con otros influencers de confianza en caso de ciberataques.

Sección 2: Streaming

El streaming se ha convertido en una forma popular de consumir contenido en línea. Aquí te presentamos algunos aspectos importantes a considerar:

Definición y Funcionamiento del Streaming: El streaming permite compartir y enviar contenido multimedia en tiempo real. No es necesario descargar el contenido previamente, ya que las plataformas de streaming cargan automáticamente los archivos después de la transmisión.

Tendencias y Rankings en el Streaming: Conoce las tendencias actuales y los tipos de contenido más consumidos a través del streaming. Esto incluye películas, series, música, gaming, videos on demand y podcast/webcast. Mantente al tanto de lo que está en boga para ofrecer contenido relevante a tu audiencia.

Sección 3: Influencers

El mundo de los influencers está en auge, pero también conlleva ciertos riesgos. Aquí hay algunas consideraciones importantes:

Importancia de la Seguridad para los Influencers: Los influencers pueden ser blanco de ataques informáticos que comprometen su credibilidad y la confianza de su audiencia. Por lo tanto, es fundamental tomar medidas para proteger tus datos y mantener la integridad de tu imagen.

Verificación de Integridad de la Cuenta: Verifica regularmente la integridad de tu cuenta y utiliza plataformas que permitan la verificación de identidad. Esto ayudará a construir confianza con tu audiencia y establecer tu legitimidad en el mundo del influencer.

Definición de streaming: El streaming es el envío y recepción de datos en un flujo continuo a través de una red informática, desde un servidor remoto hasta un dispositivo. Permite la reproducción de contenido mientras los datos se están transmitiendo.

Uso y popularidad del streaming: El streaming se ha vuelto habitual en nuestro día a día como ciberusuarios. Esta tecnología nos permite compartir contenido multimedia en tiempo real sin necesidad de descargarlo. Puede llevarse a cabo en vivo o grabado. En 2020, debido a la pandemia de COVID-19, hubo un aumento del uso de servicios de streaming, con un incremento del 71% en las cifras de audiencia con respecto al año anterior.

Riesgos de ciberseguridad del streaming: Es importante conocer los riesgos asociados al streaming en línea para evitar ciberataques como el malware, el phishing y la piratería informática. Los ciberdelincuentes aprovechan los sitios de streaming en línea como un mercado lucrativo para lanzar ataques y robar información personal y financiera.

Medidas de seguridad recomendadas: Para disfrutar del streaming de manera segura, se recomienda mantener los sistemas actualizados, contar con soluciones de seguridad instaladas y estar al tanto de los riesgos. También es importante configurar y ajustar la privacidad de las cuentas, prestar atención a los enlaces compartidos en los chats y corroborar la legitimidad de cada aplicación.

Plataformas y contenido más populares: Algunas de las plataformas más utilizadas para el streaming son YouTube, Twitch, Pluto TV, Tubi y Crackle. En cuanto al contenido, las películas, series, música, videojuegos, deportes y conciertos son los más consumidos a través del streaming.

Consejos adicionales para influencers: Si eres un influencer o una figura pública que utiliza el streaming, se sugiere verificar la integridad de tu cuenta para evitar filtraciones de datos. También se recomienda tener moderadores para regular la interacción de la comunidad.

Ciberseguridad para un streaming confiable

Actualmente, el streaming ocupa gran parte del mundo virtual. Veamos qué es y cómo usarlo (o practicarlo) de manera segura.

Compartir en Redes

El streaming se ha convertido en algo habitual dentro de nuestro día a día como ciber-usuarios/as.

Esta tecnología permite compartir y enviar, a un servidor y en tiempo real, contenido multimedia, destinado a ser consumido por los/las usuarios/as, sin tener que descargarlo.

Lo interesante es que puede llevarse adelante tanto en vivo como grabado. En caso de que sea en vivo, muchas de las plataformas cargan el contenido audiovisual automáticamente, una vez finalizado el streaming.

El uso de esta herramienta permite conectarnos e interactuar con comunidades, ver nuestras películas y series favoritas, compartir habilidades en videojuegos, escuchar música y hasta presentar un lanzamiento de un producto o evento, entre otros.

Puntos clave si queres stremear:

Contar con una conexión estable a Internet.
Seleccionar correctamente la plataforma según tu contenido, audiencia y estilo.
Elegir si el contenido es creado en vivo o grabado.
Tener moderadores que regulen la interacción de tu comunidad.

Puntos clave si sos suscriptor/a:

Verificar que las plataformas sean legítimas y confiables.
Configurar y ajustar la privacidad de tus cuentas.
Prestar atención a enlaces compartidos en los chats.
Saber que no es necesario descargar el contenido para reproducirlo.

Ranking de lo más consumido vía streaming:

Películas / Series
Música
Gaming / eSports / IRL (In Real Life)
Videos On Demand (deportes, conciertos, etc.)
Podcast / Webcast

Ranking de las plataformas gratuitas más utilizadas:

YouTube
Twitch
Pluto TV
Tubi
Crackle

Al disfrutar de estas plataformas, recordemos que, es importante tomar ciertos recaudos como, por ejemplo: configurar correctamente nuestros datos en las cuentas y corroborar la legitimidad de cada aplicación.

Riesgos de ciberseguridad del streaming en línea

Es importante conocer los riesgos de ciberseguridad del streaming en línea para remediar el riesgo de ciberataques, como el malware, las estafas de phishing y los intentos de piratería informática, que pueden poner en peligro su información personal y sus datos financieros.

La pandemia de COVID ha provocado un aumento del uso de virus vivos. servicios de streaming ya que el público buscaba nuevos contenidos continuos para mantenerse entretenido durante los paros nacionales.

En 2020, las cifras de audiencia de los servicios de streaming aumentaron un 71% con respecto al año anterior.

Los sitios de streaming en línea son un mercado muy lucrativo para que los ciberdelincuentes lancen ataques y roben información de identificación personal. Albergan datos de millones de abonados, incluidos nombres, direcciones de correo electrónico y datos de pago. El aumento de las suscripciones durante la pandemia ha supuesto un incremento sustancial del número de personas vulnerables a los ciberataques. Apenas unas horas después del lanzamiento de Disney +, las cuentas de miles de usuarios fueron pirateadas y sus contraseñas y correos electrónicos cambiados.

Los sitios de retransmisión en directo no sólo tienen masas de abonados, sino que también es habitual que los usuarios compartan sus credenciales de acceso con amigos y familiares. El hecho de compartir y reciclar contraseñas en estos sitios los convierte en un objetivo privilegiado para distribuir malware, lanzar spam y realizar ataques de phishing.

Ciberseguridad y streaming ilegal

Aunque los servicios tradicionales de streaming en línea son cada vez más populares, también hay un gran número de personas que intentan acceder a sitios de streaming con descuentos o encontrar otros métodos para ver contenidos que aún no están protegidos por derechos de autor en su localidad. Esto incluye ver contenidos ilegales desde sitios web no autorizados, a través de aplicaciones o utilizando un complemento al que se accede desde un dispositivo como un descodificador o un stick.

Aunque los usuarios pueden sentirse tentados a buscar métodos alternativos para ver sus contenidos favoritos en línea en lugar de pagar por otro servicio de suscripción, los ciberdelincuentes utilizan estos sitios web y aplicaciones ilegales para atraer a víctimas desprevenidas a estafas mediante descargas "gratuitas" de películas y programas de televisión populares.

¿Cuáles son los riesgos del streaming en línea?

Cuando se trata de aplicaciones de streaming online basadas en el entretenimiento, la seguridad suele quedar en segundo plano. Como todas las tendencias populares, el aumento del uso del streaming ha abierto un nuevo canal de ataque para los ciberdelincuentes y puede suponer un sinfín de riesgos para los usuarios. Entre ellos se encuentran:

Robo de identidad y fraude: Muchos sitios de streaming online exigen a los usuarios crear una cuenta para sus servicios. Normalmente, la gente tiende a utilizar la misma dirección de correo electrónico o nombre de usuario para todas sus cuentas. Según un estudio de Google, hasta el 65% de las personas reutilizan la misma contraseña para varias o todas las cuentas.

Si los usuarios utilizan la misma contraseña en numerosos sitios y se descubre, facilita a los piratas informáticos el acceso a otras cuentas. Los ciberdelincuentes pueden entonces extraer la información personal de los usuarios y venderla a terceros, poniendo a los usuarios en riesgo de robo de identidad y estafas.

Una investigación encargada por FACT reveló que casi la mitad de los encuestados estarían dispuestos a compartir su dirección de correo electrónico personal para acceder a un flujo ilícito.

Malware: Muchos sitios ilegales de streaming en línea están plagados de malware o adware disfrazados de archivos de vídeo pirateados.

El software malicioso puede infectar otros dispositivos conectados a una red y dar a los piratas informáticos acceso directo a los archivos privados de un dispositivo. El software malicioso también puede ralentizar el dispositivo o hacer que no responda, mostrar ventanas emergentes o anuncios, o llevarle a sitios que no desea visitar.

Phishing: las estafas de phishing suelen imitar las páginas de inicio de sesión de las plataformas de streaming o enviar correos electrónicos falsos que parecen proceder de servicios de streaming populares, para engañar a los usuarios y que confirmen sus datos de pago o añadan su información de facturación.

Si los destinatarios introducen sus credenciales, los ciberdelincuentes pueden utilizar su información sensible para realizar futuros intentos de phishing, obtener acceso a otras cuentas o recuperar la información de la tarjeta de crédito vinculada a la cuenta.

Contenido inapropiado: Ver contenidos a través de un sitio web no autorizado, una caja modificada, un stick o un complemento puede exponer a los espectadores más jóvenes a anuncios explícitos ycontenidos inapropiados para su edad.

Cómo mantenerse seguro en Internet mientras se transmite

Utiliza servicios de streaming legales: Hay muchos servicios de streaming legales disponibles, como Amazon Prime, Netflix y NOW TV. Estos servicios de "vídeo bajo demanda por suscripción" (SVOD) han ido ganando popularidad en los últimos años y cuentan con aplicaciones y sitios web limpios y dedicados, sin amenazas de malware o adware.

Los servicios de SVOD suelen tomar medidas de seguridad reforzadas para mantener los datos de sus abonados a salvo, entre ellas:

Cookies seguras para evitar el malware

Protección DNS para verificar la autenticidad de las direcciones de correo electrónico de los usuarios

Robustos algoritmos SSL para el cifrado de datos

Evita compartir datos con plataformas que no sean de confianza: Nunca debes compartir tus datos personales con sitios desconocidos o apps que no conozcas o en las que no confíes.

No haga clic en enlaces sospechosos: Los ciberdelincuentes suelen incrustar programas maliciosos en imágenes o hipervínculos camuflados. Nunca hagas clic en enlaces o avisos de descarga sospechosos.

Protección por contraseña: Utiliza una contraseña segura, que incluya letras minúsculas y mayúsculas, números y símbolos. No utilices nunca la misma contraseña en todas tus cuentas.

Twitch: riesgos y particularidades del streaming en vivo

busca acompañar madres, padres y docentes en el cuidado de los niños en Internet con el fin de generar conciencia acerca de riesgos y amenazas en el mundo digital, analiza el fenómeno Twitch y acerca los puntos claves sobre la nueva plataforma streaming de video en vivo y cuidados que hay que tener al utilizarla.

Twitch es una plataforma de streaming de video en vivo. En otras palabras, permite que los usuarios vean o transmitan el desarrollo de alguna actividad mientras interactúan con otros usuarios en tiempo real. Fundada en 2011 y adquirida por Amazon en 2014, Twitch alcanzó sorprendentes números de visitas durante los primeros meses de 2020: únicamente entre enero y julio, se ha contabilizado un total de 639 billones de minutos de visualización, de acuerdo con el sitio TwitchTracker. Tiene un promedio que supera los 2 millones de espectadores diarios y hay más de 6 millones de streamers (quienes transmiten) por mes.

Además de ser un sitio al que puede ingresarse desde cualquier computadora, Twitch tiene aplicaciones para iOS y Android, y permite el acceso desde consolas como Xbox y PlayStation. Se trata de un servicio gratuito (con publicidad) que no requiere de una suscripción para ingresar, y una vez dentro ofrece la posibilidad de interactuar, transmitir o simplemente ver lo que otro/as transmiten. Ocho son las categorías de contenido disponibles: música; talk shows y podcasts; deportes; aire libre y viajes; comida y bebida; charlando; eventos especiales; y la más popular de todas, juegos.

Seguridad y aspectos a tener en cuenta

La edad mínima requerida para crear una cuenta en el sitio es de 13 años (con supervisión de adultos recomendada hasta las 18), lo que puede alterarse con solo ingresar una fecha de nacimiento falsa. Si bien no es necesario crear una cuenta para acceder al contenido, hacerlo le permitirá al usuario realizar sus propias transmisiones y recibir alertas cuando algún streamer de su interés haya iniciado su transmisión.

Cada una de las transmisiones de Twitch incluye la función de chat, que, si bien puede ocultarse, no es posible eliminarla. En ocasiones este espacio solo está habilitado a ciertos usuarios, como los seguidores o suscriptores del streamer, pero aun así es posible ver lo que otros publican. Existe además la opción de que un usuario se contacte de forma directa con otro mediante mensajes directos, conocidos como Whispers. Cabe mencionar que la plataforma ofrece la opción de limitar quién puede contactarnos, configurable desde el menú de Ajustes, y permite bloquear o denunciar usuarios directamente desde el chat.

De acuerdo a una investigación de Wired, varios de los/as niño/as menores de 13 años que fueron identificados en la plataforma y que realizaban transmisiones recibían por estos medios mensajes inapropiados de participantes anónimos, en ocasiones solicitando datos de contacto como el número de WhatsApp o perfil de redes sociales. “Estar atentos al uso que los niño/as hacen del sitio, y de Internet en general, será crucial para evitar que experimenten situaciones incómodas en línea, como puede ocurrir si se encuentran ante una hecho de ciberbullying o grooming.”,comentó Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Por otro lado, es importante saber que, si bien el acceso al servicio es gratuito, Twitch incluye gastos dentro de la plataforma como puede ser a través de la compra de Bits, la moneda de Twitch, que los usuarios pueden adquirir para apoyar a sus streamers favoritos; por medio de

donaciones a dichos streamers; o mediante suscripciones pagas para acceder a contenido exclusivo. Desde ESET se recomienda conocer el uso que los niño/as hacen de la plataforma para evitar estafas, en ocasiones incitadas por otros usuarios a través del chat, o gastos indeseados, a veces promovidos incluso por los propios streamers, aprovechando el fanatismo que despiertan.

En cuanto a control parental, no existe una configuración especifica en Twitch y tampoco es posible bloquear transmisiones ni limitar el tiempo de uso desde la plataforma, aunque siempre estará la posibilidad de hacerlo en forma directa con los más pequeños, o aprovechar otras herramientas generales, como ESET Parental Control. Por otro lado, si bien la plataforma tiene normas rígidas respecto de, por ejemplo, la publicación de contenido sexual, no ofrece filtros por edad para los videojuegos, que muchas veces incluyen desnudos o contenido violento. Sí existen etiquetas, que pueden actuar como filtro, aunque son los propios streamers quienes deben agregarlas a su contenido. Lo mismo ocurre con los mensajes enviados en el chat público; algunos streamers establecen reglas, que aparecen solo como un pequeño cuadro de diálogo al querer escribir un mensaje, pero no evita que el usuario escriba lo que desee. También son ellos quienes tienen la posibilidad de determinar que un contenido es únicamente para adultos, aunque basta con seleccionar “Ver contenido” para ingresar a la transmisión.

“Como madre o padre, es importante mantenerte actualizada/o acerca de las tendencias del mundo digital, aún más si son tus niños/as quienes se ven involucrados. Sí, existen formas de mantenerlos protegidos en la plataforma Twitch, pero no debe perderse de vista la esencia del streaming en vivo: no hay filtros ni ediciones al contenido que se transmite en tiempo real, y eso lo vuelve impredecible. También es importante recordar que, más allá de los videojuegos, hay múltiples transmisiones disponibles en las otras categorías mencionadas que ofrecen material educativo y/o artístico, para aprender o disfrutar de la música, la cocina, las artes plásticas y más. Los riesgos existen, y ser conscientes de ello es el primer paso para mantenerse seguros en el mundo digital. Mantener los sistemas actualizados, contar con soluciones de seguridad instaladas, y estar al tanto de los riesgos nos permiten disfrutar de la tecnología de manera segura“, aconseja Gutiérrez Amaya.

¿Qué significa el streaming?

El streaming es enviar y recibir datos en un flujo continuo a través de una red informática, desde un servidor remoto hasta un dispositivo. El streaming en línea permite que se inicie la reproducción de contenido mientras el resto de los datos todavía se está enviando al dispositivo.

Cuando transmita contenidos por Internet, en cuanto el ordenador o el teléfono empiecen a recibir los datos, podrá empezar a ver el programa, la película o cualquier otra cosa que esté transmitiendo. Mientras el contenido de vídeo o audio sigue reproduciéndose, el resto de los datos se transmiten al dispositivo de forma gradual. Cuando hace streaming, puede empezar a consumir contenidos al instante, sin tener que esperar a descargar todo el archivo.

El streaming se suele utilizar para el audio, el vídeo y los juegos. Siempre que tenga una conexión a Internet fiable, el dispositivo podrá reproducir toda la película o el programa correctamente y sin interrupciones. Cada vez que ha usado servicios de música como Spotify o Apple Music, reproductores de vídeo como YouTube o Netflix, aplicaciones como Twitch o algunos tipos de juegos en línea, ha visto el streaming en acción.

¿Cómo funciona el streaming?

El streaming funciona descomponiendo el contenido (por ejemplo, una película) en pequeños fragmentos o paquetes de datos. Estos paquetes de datos se envían al navegador, donde el reproductor de vídeo interpreta los datos como una película. Cuando el navegador tiene suficientes paquetes de datos para comenzar, la película empieza a reproducirse.

La mayoría de los sitios de streaming utiliza capas TCP/IP (protocolo de control de transmisión/Internet) estándar en lugar de UDP (protocolo de datagramas de usuario) para transmitir contenido de un servidor a un dispositivo. El protocolo TCP/IP es más fiable para hacer llegar los paquetes de datos a donde deben ir y en el orden correcto. Sin embargo, los sitios de streaming que se basan en UDP suelen ofrecer transferencias más rápidas. Netflix, Amazon Prime y Spotify utilizan TCP, mientras que YouTube usa una combinación de TCP y UDP.

Las empresas que ofrecen contenido en streaming también necesitan servidores o plataformas en la nube para el almacenamiento. Las grandes empresas como Netflix tienen redes de envío de contenido que conservan el contenido más popular en caché y geográficamente cerca del punto adonde se transmitirá. Esto reduce los costes del ancho de banda y la latencia, y hace que sea más sencillo ver la TV en línea.

Para que el streaming funcione, es imprescindible disponer de una conexión a Internet fiable y con velocidad suficiente. Deberá ser de 2 Mbps (megabits por segundo) como mínimo para proporcionar una buena experiencia de streaming sin retrasos ni reducciones de la calidad. Si la conexión es demasiado lenta, se producirán pausas constantes mientras el dispositivo almacena en búfer. Si desea ver contenido en HD o 4K, debería disponer de una conexión aún más rápida, de 5 Mbps como mínimo.

Cuando transmite en línea, el contenido (por ejemplo, una canción o un programa de TV) se descompone en pequeños paquetes de datos que se envían al navegador.El streaming le permite ver programas en línea sin tener que esperar a que se descargue un archivo por completo.

¿En qué se diferencia el streaming de las descargas?

La diferencia entre el streaming y la descarga es que, cuando se descarga una película o una canción, el archivo completo se guarda en su dispositivo. Cuando finaliza la descarga, puede empezar a verla o escucharla. En cambio, la definición de streaming es que puede reproducir contenido multimedia sin descargar un archivo.

Las principales ventajas de la descarga son que no tendrá problemas de almacenamiento en búfer y que podrá guardar sus contenidos favoritos. No obstante, si descarga todo el contenido, especialmente archivos multimedia de gran tamaño como películas en HD, llenará enseguida todo el espacio disponible en el disco duro.

Aunque el streaming puede ser complicado a veces si tiene una conexión lenta a Internet, el contenido nunca ocupa espacio. Además, con la gran cantidad de opciones de streaming disponibles (servicios de música como Spotify y Apple Music, reproductores de vídeo como YouTube, Netflix, Hulu y HBO Max, plataformas sociales de streaming como Twitch y muchos juegos y aplicaciones) transmitir es más fácil que nunca.

¿Qué es el almacenamiento en búfer?

El almacenamiento en búfer se produce cuando los datos de audio o vídeo se cargan previamente en la reserva de memoria (búfer) del reproductor multimedia al transmitir contenidos en línea. El almacenamiento en búfer asegura que, si tiene lugar una breve interrupción en la conexión, podrá seguir transmitiendo los datos que ya se han recogido en el búfer.

Ahora bien, si la conexión a Internet es demasiado lenta, el reproductor puede dejar de almacenar contenido en el búfer, lo que significa que ya ha transmitido el contenido recopilado previamente. Es posible que deba esperar varios segundos o minutos para volver a acumular suficiente contenido en el búfer y continuar con la reproducción.

¿Qué tipo de contenidos se pueden transmitir?

Puede transmitir muchos contenidos en línea. El audio y el vídeo son las formas más tradicionales de streaming, incluidos la música, los podcasts, los programas de TV, los libros y las películas. Cada vez se pueden transmitir más tipos de juegos y eventos en directo a través de aplicaciones móviles, navegadores y otros reproductores multimedia.

Música y otro audio

El streaming de audio, incluidos la música y los podcasts, se ha vuelto increíblemente popular. Los servicios de música en streaming le permiten reproducir montones de canciones de diferentes artistas, todo ello sin tener que descargar ni un solo archivo.

Los servicios como Spotify, Pandora y Apple Music proporcionan millones de pistas disponibles en streaming con solo tocar un botón. Algunos sitios de streaming, como Pandora, permiten escoger un género o un estado de ánimo, y se encargan de seleccionar las listas de reproducción. Otros, como Spotify, reproducen exactamente lo que ha elegido, aunque las listas de reproducción también son un componente importante de la plataforma. Apple Music ofrece una mezcla de ambas opciones.

Los podcasts se pueden transmitir o descargar para escucharlos más tarde, y están disponibles mediante servicios como iTunes, Stitcher o Audible. También puede transmitir archivos de

audio usted mismo a otros dispositivos (por ejemplo, desde su teléfono para reproducir archivos de audio a través de su altavoz Bluetooth) en su hogar.

Vídeo

El vídeo fue el primer éxito masivo de streaming y comenzó con servicios como YouTube. En lugar de tener que descargar grandes archivos multimedia, el streaming de vídeo comprime los datos en pequeños paquetes y los envía a su dispositivo, donde se descomprimen y se reproducen.

Durante una sesión de streaming, el vídeo se guarda en el búfer constantemente; mientras está viendo un paquete de datos, el siguiente paquete se está descomprimiendo para que pueda ver toda la película o el programa sin interrupciones.

Actualmente, algunos de los servicios de streaming de vídeo más populares son YouTube, Netflix, HBO Max, Amazon Prime, Hulu, Google Play y Disney+.

El vídeo en streaming le ahorra mucho tiempo y molestias. En lugar de descargar grandes archivos, que ocuparían mucho espacio de almacenamiento en su dispositivo, puede ver lo que desee sin tener que guardar nada.

Sin embargo, podría tener problemas si trata de transmitir sus contenidos favoritos desde el extranjero. Muchos sitios bloquean según la ubicación, lo que significa que restringen ciertos contenidos a determinadas áreas. Si está de viaje y desea acceder a sus contenidos favoritos de su país, podrá seguir haciéndolo, pero tendrá que usar una VPN.

Una VPN protege todo el tráfico de Internet hacia y desde su ordenador enviándolo a través de un túnel cifrado.Una VPN envía su tráfico de Internet a través de un túnel cifrado.

Una VPN cifra su conexión y le permite ocultar su dirección IP y elegir dónde quiere que aparezca el dispositivo. Así, puede establecer su ubicación en otro país y esquivar las restricciones geográficas y otros bloqueos de contenidos.

Juegos y aplicaciones

El juego en streaming o en la nube funciona como el streaming de audio o vídeo. Ahorra espacio y recursos de procesamiento en el dispositivo descargando los contenidos en el servidor de juegos de una empresa.

Cuando juega en streaming, básicamente está enviando comandos a un ordenador más potente que los ejecuta y transmite el resultado de vuelta a su dispositivo. En los últimos tiempos, la velocidad de Internet ha aumentado lo suficiente para hacer este proceso factible en tiempo real.

Apple ofrece ahora algunos juegos que solo incluyen funciones básicas en su descarga, después envían por streaming los nuevos niveles u otro contenido a medida que los usuarios lo necesitan mediante un proceso llamado recursos bajo demanda. Asimismo, Xbox Cloud Gaming es un servicio de juego en streaming que le permite utilizar cualquier dispositivo que pueda acceder a un navegador para jugar; sin necesidad de discos, descargas ni consolas.

Se están desarrollando otros servicios de juegos y aplicaciones en streaming. Además, según sus necesidades, el uso de una VPN para jugar tiene sus ventajas, por ejemplo en juegos como el GTA 5 o en otros de alta exigencia.

¿Qué es el streaming en vivo y cómo funciona?

El streaming en directo funciona de forma parecida al de otros tipos de contenido, pero se usa para eventos especiales, como deportes, conciertos o debates políticos. Mientras la está viendo, la transmisión se guarda temporalmente y se muestra en pequeñas cantidades de datos en su dispositivo. Después, se descartan a medida que continúa.

Cuando ve una transmisión en vivo, visita un sitio web (como un sitio de noticias o de deportes) alojado en un servidor web. Este servidor web se conecta a un servidor de medios, que envía el contenido a su dispositivo usando el protocolo de transporte en tiempo real (RTP por sus siglas en inglés) y el protocolo de transmisión en tiempo real (RTSP). Esos protocolos permiten que los archivos de vídeo se envíen en un formato más pequeño (comprimido) y luego se vean con mayor calidad (descomprimidos) en su dispositivo.

Como sucede con cualquier otro tipo de streaming, cuando ve un streaming en vivo, nunca recibe el archivo; solo las partes que necesita en cada momento para su reproducción en vivo. Las plataformas de redes sociales ahora ofrecen elementos de streaming en directo, como Facebook Live o Instagram Live.

¿Por qué debería usar la transmisión de contenidos?

El streaming de contenidos es muy cómodo en casi todos los sentidos. A continuación, se enumeran algunas de sus principales ventajas:

Consiga una reproducción instantánea: sin tener que esperar a que se descargue el contenido. El streaming le permite empezar a ver o escuchar casi de inmediato.

Evite altos costes y el pirateo: Comprar un CD o una descarga digital de cada banda que le gusta resulta muy caro. Y descargar contenido protegido por derechos de autor de sitios de torrent es ilegal. Puede acceder a todo el contenido que desea por una cuota mensual reducida de un servicio de streaming.

Ahorre espacio: a diferencia de la descarga, el streaming no guarda archivos de gran tamaño en su dispositivo. Tiene acceso a grandes cantidades de música y películas sin llenar su disco duro.

Acceda a contenido en vivo: ¿desea ver acontecimientos importantes en directo, como debates políticos, partidos o incluso el Festival de Eurovisión, pero no tiene un televisor? El streaming en directo le proporciona acceso a través de su portátil u otros dispositivos.

Acceda a contenido desde el extranjero: ¿está de viaje en el extranjero y desea ver sus programas de televisión favoritos de su país? una de las ventajas de una VPN que puede cambiar la dirección IP para transmitir su contenido favorito de su país de origen cuando está de viaje.

Cómo mejorar la experiencia de streaming

¿Tiene dificultades para transmitir su contenido favorito? A continuación, encontrará algunas formas de mejorar la transmisión en su ordenador, teléfono u otro dispositivo:

Potencie su Wi-Fi: necesita una conexión a Internet lo suficientemente rápida para transmitir correctamente. Intente potenciar la intensidad de la señal Wi-Fi de su hogar para mejorar la velocidad de transmisión.

Reduzca el almacenamiento en el búfer: es posible que la velocidad de Internet no sea el único factor que provoca el almacenamiento en el búfer. Consulte nuestros consejos para reducir el almacenamiento en el búfer al transmitir.

Desbloquee opciones de streaming: ¿Está de viaje en el extranjero y sus opciones habituales de streaming están bloqueadas en su ubicación actual? Use una VPN para desbloquear los sitios web desde los que desea transmitir.

Eluda las restricciones por parte de los ISP: su ISP (proveedor de servicios de Internet) puede limitar la velocidad de Internet si observa que está usando mucho ancho de banda. Use una VPN para eludir las restricciones por parte de los ISP y transmitir tanto como desee.

Protéjase mientras transmite en una red Wi-Fi pública: aunque ponerse al día con los programas puede ser una muy buena forma de pasar el tiempo durante una escala en el aeropuerto, existen algunos riesgos al usar una Wi-Fi pública. Utilice una VPN para protegerse mientras transmite contenido en una red Wi-Fi pública.

Limpie su dispositivo: su ordenador puede tener dificultades para transmitir si está atascado con archivos no deseados y otros restos digitales. Trate de limpiar el PC o de acelerar el Mac para conseguir un mejor rendimiento general.

Asegúrese de que dispone de suficiente memoria: Si carece de suficiente RAM (memoria de acceso aleatorio), el ordenador puede tener dificultades para transmitir si está usando varias aplicaciones a la vez. En casos poco comunes, incluso puede que deba actualizar su RAM para conseguir un mejor rendimiento en streaming.

Optimice su PC para juegos: tanto si desea transmitir juegos como jugar en línea, siempre es una buena idea potenciar su equipo de juego para conseguir una experiencia de juego óptima.

¿El streaming tiene inconvenientes?

Un posible inconveniente del streaming es que depende de una conexión a Internet rápida y estable. Si no dispone de una buena conexión a Internet, o de suficiente ancho de banda, la retransmisión será difícil. El contenido puede pausarse o entrecortarse mientras intenta finalizar el almacenamiento en búfer, lo que supondrá una interrupción del visionado o la escucha.

Según el servicio de streaming que utilice, la calidad puede ser incoherente. Si el acceso Internet es inestable, puede ocurrir que el programa de TV comienza y se detiene, se ve borroso, o que la imagen y el sonido se desincronizan. Si está acostumbrado a los Blu-Ray de alta calidad, notará una disminución en la calidad. Si dispone de una buena conexión a Internet, el streaming funcionará bien.

Con tantos servicios de streaming que ofrecen contenidos exclusivos, los costes pueden aumentar rápidamente si se mantienen varias suscripciones a la vez. Puede que le preocupen el seguimiento en línea, la recopilación de datos y la cantidad de información personal que pueden recoger las empresas interesadas en saber sus preferencias de escucha y visionado.

Los servicios de streaming también han estado en el punto de mira de los artistas, que se quejan de que las plataformas les dificultan obtener una compensación adecuada por su trabajo. Tidal, la plataforma de música en streaming propiedad de Jay-Z, es un servicio que intenta compensar a los artistas de forma más justa por los contenidos en streaming.

¿Existen riesgos de seguridad al transmitir?

Existen algunos riesgos de seguridad al transmitir, sobre todo al usar sitios web de streaming que no son de confianza. Si bien los grandes nombres como Netflix y Spotify son seguros, existen muchos sitios de streaming sospechosos.

¿Cómo saber si ha aterrizado en un sitio de streaming inseguro? Si el sitio no es muy conocido, pero ofrece una buena cantidad de películas y programas de TV populares, podría estar emitiéndolas de forma ilegal (pirateadas). Si el sitio dispone de los títulos más recientes, como películas que aún están en cartelera, probablemente estén pirateados.

Otro signo de advertencia es el bombardeo de montones de anuncios en su dispositivo cuando visita el sitio de streaming. Estos anuncios pueden estar mezclados con software malicioso, que puede infectar su dispositivo en cuanto aparecen. Trate de usar un bloqueador de anuncios para impedir que se carguen estos anuncios.

Si no está seguro de si un sitio es legítimo o no, es aconsejable buscar «[sitio de streaming] + comentarios» o «es [sitio de streaming] legítimo». También debería prestar atención a otros indicadores de sitios web inseguros. Y protegerse de descargas maliciosas, virus y otros tipos de malware con una potente herramienta de eliminación de malware y análisis de virus.

Permanezca seguro y en el anonimato mientras realiza streaming

El hecho de que no descargue archivos a su dispositivo cuando utiliza el streaming no implica que no existan riesgos. Como mencionamos anteriormente, es importante asegurarse de que está usando un sitio legítimo que posee las licencias adecuadas para el contenido.

Además, puede usar una VPN para cifrar su conexión y mantener su privacidad en línea. Las VPN le permiten cambiar fácilmente su ubicación (virtual), lo que evita que los servicios de streaming y los anunciantes lo aborden según el lugar donde esté.

Usar una VPN puede ayudarle a proteger su privacidad y sus datos cuando transmite en línea.Usar una VPN al transmitir le permite acceder a contenido que no está disponible en su ubicación.

Si está de viaje en el extranjero y desea acceder a programas de su país o bien desea permanecer seguro en redes Wi-Fi públicas, AVG Secure VPN mantendrá sus actividades en línea protegidas y en privado.

Ciberseguridad y Privacidad para Influencers

En un mundo lleno de riesgos tanto físicos como informáticos, la integridad, disponibilidad y confidencialidad de nuestros datos son uno de los desafíos más críticos. Estos factores no solo impactan nuestra privacidad, sino que también afectan nuestra imagen frente al público. La presente guía se centra específicamente en tips/consejos fundamentales para influencers, aquellos que buscan convertirse en uno o para el público en general.

Ciberseguridad y Privacidad para Influencers

La importancia de que los influencers se tomen en serio la seguridad de sus datos radica en varios incidentes del pasado, donde personajes públicos, influencers y empresas han sido víctimas de varios tipos ataques informáticos, en especial la suplantación de identidad. Estos ataques no solo comprometen la credibilidad de la figura pública afectada, sino que también repercuten en la confianza de su audiencia. Es crucial comprender que, aunque la imagen del influencer o personaje público sea el blanco directo de estos ataques, el principal objetivo de los atacantes es el público mismo. Engañar a cuantas personas sea posible, ya sea mediante estafas con criptomonedas o phishing (envío de mensajes falsos que pretenden ser confiables para engañar a los usuarios y obtener datos personales o financieros).

Para evitar caer en estos riesgos, es esencial que los influencers, como figuras con alcance a miles o incluso millones de personas en las redes sociales, asuman la responsabilidad de proteger sus cuentas y datos, ya que actualmente no se trata únicamente de individuos con 50 o 1000 seguidores, sino de personajes que tienen un impacto masivo gracias a la viralidad en las diversas redes sociales.

Tips: Ciberseguridad y Privacidad para Influencers

Si eres un influencer, una figura pública, quieres convertirte en uno o simplemente buscas un mejor control de tus datos, esta guía está diseñada para ti. Incluso si no encajas en estas categorías, compártela con aquellos que puedan beneficiarse de esta información.

1 – Verificación de Integridad de la Cuenta (filtración de datos).

“¿Me han hackeado mi cuenta?”, un término mal dicho, más bien, ¿han sido filtrados mis datos?

Antes de crear una cuenta o si ya la tienes, verifica que tu correo o teléfono no haya sido comprometido. Puedes usar plataformas como ‘;–have i been pwned para comprobar, es tan fácil como abrir el sitio web y escribir tu correo o incluso tu teléfono móvil.

Verifica si tus datos están expuestos _> https://haveibeenpwned.com/

Ejemplo: test@gmail.com

Si sale Oh no – Pwned (color rojo), es un mal indicador, quiere decir que en algún momento nuestra cuenta fue filtrada a internet y en algunos casos si seguimos bajando vas a poder ver de que sitios o plataformas fueron extraídos ilegalmente nuestros datos (sea por negligencia de protección de datos de las plataformas, o simplemente porque nada es seguro).

Si sale Good news — no pwnage found! (color verde), es un buen indicador, ¡pero no te confíes, sigue leyendo la guía!

2 – Uso de Contraseñas Robustas y Únicas

Asegúrate de que tus contraseñas cumplan con las mejores prácticas de seguridad.

Ejemplo: Uso de mayúsculas, minúsculas, símbolos y números.

Contraseña insegura

Contraseña segura (es un ejemplo, no la usen, justo en este momento se ha vuelto insegura por enseñarla).

Esto es un claro ejemplo de que las contraseñas por muy complejas que sean, si son enseñadas a alguien por equivocación o filtradas en internet, dejan de ser seguras.

Por ello también recomiendo que las contraseñas sean únicas para cada sitio o servicio en el que nos registramos.

Herramienta usada para el ejemplo:> https://password.kaspersky.com/es/

3 – Uso de Autenticación de Doble Factor (2FA) o MFA

No se debe confiar en las contraseñas únicamente para iniciar sesión en una plataforma, por ello es recomendable el uso de métodos extras para protegerte los cuales una vez intentes iniciar sesión te pedirá un código para verificar que eres tú realmente el que está realizando esta acción.

Es recomendable que estos métodos sean exclusivos de aplicaciones creadas para esta función y no de mensajes de voz o verificación por SMS. Algunas aplicaciones más conocidas son: Authy, Google Authenticator, Microsoft Authenticator, entre muchos otros, No nombro todos los existentes para no entrar en detalles técnicos.

Algunas plataformas ya por defecto te piden activar las cuentas mediante estas opciones, pero no todas, así que para configurarlo la mayoría de aplicaciones siguen este patrón: Cuenta, seguridad, opciones de seguridad, activar 2FA o MFA.

Recursos:

Cómo funciona la autenticación en dos pasos en Facebook – https://es-es.facebook.com/help/148233965247823

Usar una app para la autenticación en dos pasos en Instagram – https://help.instagram.com/1582474155197965?locale=es_LA

Cómo activar la Verificación en 2 pasos en Google – https://support.google.com/accounts/answer/185839?hl=es-419&co=GENIE.Platform%3DAndroid

Activa la verificación en dos pasos en TikTok – https://support.tiktok.com/es/safety-hc/account-and-user-safety/account-safety

Configurar la autenticación en dos pasos (2FA) en Twitch – https://help.twitch.tv/s/article/two-factor-authentication?language=es

4 – Uso de Gestores de Contraseñas

El uso de gestores de contraseñas es una buena opción a la hora de gestionar este tipo de datos de seguridad, unos de los beneficios son:

Evitar tener todo registrado en un papel que alguien fácilmente puede encontrar.

Es un complemento para todas los tips que he nombrado anteriormente.

Establecer una contraseña segura.

Gestionar todos los sitios donde tienes tus datos.

Comprueba si tus cuentas o contraseñas están filtradas en internet.

Los gestores de contraseñas son a elección de cada uno, lo que si no recomiendo es usar gestores de contraseña integrados por defecto en el navegador, me refiero al típico mensaje, quieres guardar tu contraseña en Google para futuro uso, Firefox, entre otros…

Para ello existen las siguientes alternativas:

https://proton.me/pass

https://bitwarden.com/

https://www.lastpass.com/es

https://1password.com/es

Existen muchos más, con mejor seguridad, sin reporte de incidentes, pero complicaría técnicamente la guía.

5 – Separación de Cuentas de Correo

Es aconsejable separar las cuentas de correo debido a que en cualquier momento pueden filtrarse tus datos por parte de un servicio en el que estés registrado o te roben tus contraseñas, esto ayudaría a que la cuenta robada solo funcione para un servicio en específico y no para todos dependiendo del uso que le des a cada una, ejemplo: para redes sociales, bancos y educación. Aunque puede ser complicado, el tiempo invertido será insignificante comparado con el tiempo necesario para recuperarte si eres victima un robo de datos.

Ejemplo:

Caso 1: Facebook = influencerfacebook@mail.com – TikTok = influencertiktok@mail.com

Caso 2: Redes Sociales = redesinfluencer@mail.com – Personal = privadoinfluencer@mail.com

6 – Concientización sobre Posibles Riesgos

Al ser un influencer, estarás expuesto a diversos tipos de ataques. Desconfía de todo tipo de mensajes u ofertas de trabajo tentadoras, ya que podrían incluir archivos o software maliciosos.

Ejemplo 1: El típico mail que te llega con una oferta informándote que les gusta mucho tu marca personal y que quisiera que colaboras con ellos, en este caso te pedirán que descargues un archivo PDF/Word con la oferta o el software que quieren que pruebes. Con esto no solo obtendrían acceso a tus cuentas, sino a tus dispositivos.

Ejemplo 2: Felicitaciones has sido elegido por toda la comunidad para los premios Super Influencer por favor envíanos tus datos… (Luego te harán pagar por algunos tarifas y adicional roban tus datos privados).

7 – Restringir Permisos a tus Colaboradores

En algunas ocasiones por falta de tiempo, por ahorrarnos trabajos técnicos o creativos, le otorgamos permisos sobre nuestras cuentas a colaboradores, amigos o familia.

Este tipo de permisos tenemos que revisarlo muy bien, ya que algunas de estas personas pueden estar siendo víctimas de un ciberataque desde hace mucho sin darse cuenta, o puede que le den cero importancia a la seguridad.

Por eso, antes de darle permiso sobre nuestras cuentas, verifica con ellos que se preocupen por estos temas, no tiene que ser un experto, solo cumplir con requisitos mínimos que he ido nombrando en toda la guía y si es posible que realicen la parte creativa, técnica y tú te encargas de publicar o gestionar tu propio contenido.

8 – Cuidado con el Software Pirata

Muchos creadores de contenido, al principio de su carrera o incluso hoy en día con millones de seguidores, hacen uso de software pirata, esto porque para la edición de videos, audio o imágenes tienden a usar herramientas populares como Adobe u otras herramientas que su licenciamiento son bastante costosas, o incluso el mismo Windows. Para ello recurren a instalar o contratan a alguien para que les instale software pirata (con conocimiento o desconocimiento), el cual en su 99.99%, digo 101% contienen bicho o virus.

Recomendación: Paga licenciamiento si te encargas de la edición.

9 – Mantente Actualizado Sobre los Ataques Informáticos

Mantenerte al día sobre los nuevos métodos que usan los ciberdelincuentes para atacar empresas, cuentas o personajes públicos es una tarea compleja, pero para ello en las mismas redes sociales alguien que se dedique a la ciberseguridad estará al día y te lo resumirá, así que sigue a algún influencer para que estés medianamente al día (Los influencers no remplazan un medio oficial de noticias de ciberseguridad).

10 – Engagement de Tips de Ciberseguridad para tu Audiencia

Si bien no es tu nicho de mercado, lo mínimo que deberías hacer, para protegerte a ti y a tu público de posibles estafas o ciberataques, es informar o dar pequeños tips a tu audiencia, sobre:

Los riesgos del robo de identidad.

Asegurarse que un mensaje es realmente tuyo.

Asegurarse de que comprendan como se conforma tu perfil, como se escribe correctamente tu nombre de usuario, que no tienes otros nombres de usuario en la misma plataforma.

Asegurarse de que entiendan que tu no le vas a enviar un mensaje por privado pidiendo datos, fotos, dinero o ofreciendo trabajo.

Al igual que informar y solicitar a tu público que te ayuden a reportar una cuenta falsa en caso de que la identifiques o que ellos la identifiquen.

11 – Comunicación en Caso de Ataques

En caso de un ciberataque, comunícalo a otro influencer de confianza. La difusión de la noticia por parte de tus colegas puede ayudar a contener el impacto y proteger a tu audiencia. En algunas ocasiones puede ocurrir que te roben los datos y no puedas ingresar a la plataforma para comunicarlo directamente, para ello es necesario que verifiques con alguien más con el que compartas público y que te ayude a difundir lo ocurrido.

12 – Inversión en Legitimidad o Verificación

Si generas ingresos mediante tu perfil, invierte en tu legitimidad o verificación. Adquiere suscripciones en plataformas como Instagram, Facebook, X, entre otras, que otorgan insignias de verificación. Además, procura que las empresas para las en cuáles eres creador de contenido verifiquen tu identidad, esto te ayudara a apagar el fuego mucho más rápido en caso de robo de la cuenta, ya que este tipo de verificación tiene un beneficio adicional que te ayuda a gestionar, protegerte y a establecer contacto mucho más eficiente.

13 – No Descuides tus Dispositivos

Es importante que no descuides tus dispositivos en ningún tipo de casos.

Ejemplo: Si tienes visitas, si vas a un café, un coworking u otro sitio, no dejes tus dispositivos desbloqueados durante tu ausencia y si es posible cárgalos contigo, en algunos casos es posible infectar u obtener datos de un dispositivo en cuestión de minutos o incluso segundos, así que es tu responsabilidad cuidar de ellos.

14 – No uses el Wi-Fi o Cargadores Públicos

En muchas ocasiones, por la misma naturaleza de ser un influencer, requieres desplazarte o viajar grandes distancias, en las cuales probablemente no tengas conexión a internet, datos o tu batería se te quede agote, para ello existen los Wi-Fi o cargadores públicos en aeropuertos o estaciones, lo recomendable es no usarlos, ya que alguien puede estar entre medias viendo todo el tráfico o consultas que un usuario realiza e incluso robando tus datos, lo mismo ocurre con los cargadores públicos, que puede que tengan un tipo de ataque especializado para robarte los datos mediante conexión al puerto de carga.

Es recomendable antes de realizar un viaje planear muy bien si tienes cobertura o no, llevar un PowerBank extra o contratar un e-SIM para que tengas datos o internet donde viajas, también existen algunos dispositivos o Software que te ayudan a prevenir estos tipos de ataques como VPN’s y para la batería existen los Adaptadores de solo carga, pero no es lo más recomendable.

15 – Responsabilidad y Consistencia

Cumple con los consejos o tips de manera constante, ya que la ciberseguridad es un desafío continuo y personal. Las empresas son atacadas a diario, y tus cuentas podrían estar involucradas sin que lo sepas.

Estos tips requieren de tiempo y algunos se tornan un poco complejos, pero te van a ahorrar mucho más tiempo a futuro.

16 – Pregúntale a Alguien del Sector

Mantén contacto con alguien que tenga conocimientos en ciberseguridad, esto te servirá para obtener asesoramiento en el caso de que requieras comunicar alguno de estos temas a tu público y que tengas certeza de que lo que hablas está bien orientado, por casos de duda que en algún momento te llegue una oferta, que dudes de un mensaje o que sufras alguno de estos ataques, en las mismas redes sociales habrá alguien que conozca del tema y te eche una mano.

17 – Recomendación Final

Estos consejos no garantizan una protección absoluta, ya que la ciberseguridad es algo que va cambiando a diario, los ciberdelincuentes no descansan. Sin embargo, al seguir estos tips, puedes reducir tu superficie personal de ataque.