**Como Hackear una cuenta de Instagram, Facebook, TikTok, Twitter**

¿Quieres saber cómo hackear una cuenta de Instagram, Facebook, TikTok o Twitter? Bueno, en realidad funciona con cualquier red social o incluso cuentas de correo de Gmail o Hotmail, entre otros.

En este post, podrás comprobar cómo hackear una cuenta de Instagram o de cualquier red social o cuenta de correo electrónico, viendo en detalle varios métodos que funcionan y que se utilizan cada vez más por parte de los ciberdelincuentes. Y si, habéis oído bien, ciberdelincuentes. Porque entiendo que sabéis que si hackeas la red social de una persona sin su consentimiento, estás cometiendo un delito, ¿verdad?

Ahora te estarás preguntando qué porque publico este post, si lo que aparece en él no es legal. Pues la respuesta es clara. Mi principal objetivo es que todo el mundo pueda conocer los métodos que utilizan los ciberdelincuentes para intentar estafarnos, engañarnos, hackearnos. De esta forma, todo el mundo conocerá sus trampas y no caerán en ellas, o al menos, será mucho más complicado para los “malos”.

Evidentemente, en este post podrás ver y probar los métodos que funcionan, **pero es tu responsabilidad como utilices el conocimiento adquirido. Pero sin duda, vamos a ver cómo hackear una cuenta de Instagram, Facebook, Tik Tok, Twitter o lo que sea.**

Muchos pensamos que las redes sociales como tal, son muy seguras o invulnerables, como me han dicho muchas veces. Esto es así hasta cierto punto, ya que como sabéis ha habido muchas filtraciones de datos expuestas, debido a alguna brecha de seguridad. Esto es así ya que todas las redes sociales, para dar su servicio, tienen unos sistemas quepor sí mismos pueden contener vulnerabilidades y por tanto, pueden ser aprovechadas por los ciberdelincuentes para realizar un acceso no autorizado.

Esto, evidentemente es poco probable que ocurra, aunque de vez en cuando ocurre. Además, cuando ocurre, los datos obtenidos no son de carácter público, normalmente, y hay que pujar por ellos en el mercado negro, la darkweb, etc., para poder conseguirlos.

Otra cosa que debemos tener en cuenta es que nosotros mismos, podemos ser una grave vulnerabilidad para nuestros datos personales, nuestras cuentas en rede sociales, correo, etc. Y esto si es mucho más probable que ocurra. Por lo tanto, los ciberdelincuentes emplearán su tiempo en lo que puede que vayan a tener más éxito, en nosotros. Y a continuación, vamos a ir viendo los métodos más utilizados para intentar engañarnos y estafarnos, de esta forma, robarnos nuestras credenciales, es decir, nombre de usuario y contraseña, de nuestras redes sociales o cuentas de correo electrónico.

Sin más, empezamos. Vamos a ver cómo hackear una cuenta de Instagram, Facebook, Twitter, Tik Tok, Gmail, Hotmail o lo que sea.

**Método 1: Mediante la ayuda de Google ¿Será posible?**

Si entramos en Google y hacemos una búsqueda rápida de, por ejemplo, “cómo hackear una cuenta de Instagram” veremos que hay millones de resultados. Esto es así, porque la gente busca mucho estos supuestos métodos para poder hackear una red social.

Si navegamos un poco por los resultados, veremos que en todos ellos nos dicen que tienen el método infalible para hackearlas, ¿pero será cierto?

Pues nada más lejos de la realidad. Si entramos en cualquiera de los resultados obtenidos en una búsqueda en Google, veremos como en todas nos lo pueden hacer. En muchas nos solicitarán nuestros datos bancarios para proceder al cobro de los servicios, en otras nuestras credenciales de la red social en concreto para poder realizar el hackeo, y así mil combinaciones posibles. En todas ellas, saldremos perjudicados. Pagaremos y no obtendremos lo que queremos, encima les habremos dado nuestros datos bancarios o personales a los ciberdelincuentes, incluso nuestro nombre de usuario y contraseña de las redes sociales.

**Método 2: Como Hackear una cuenta de Instagram, Facebook, Tik Tok, Twitter, Gmail, Hotmail, mediante Set Toolkit**

Como vamos a ver a continuación, esto ya es otra cosa. Mediante la herramienta Set Toolkit, vamos a poder realizar acciones que nos pueden llevar a conseguir las credenciales (Nombre de usuario y contraseña) de nuestro objetivo.

Set Toolkit se trata de una suite de herramientas que nos van a ayudar a realizar un montón de tipos diferentes de ataques y estrategias a la hora de realizar por ejemplo, [phishing](https://es.wikipedia.org/wiki/Phishing), [spear-phishing](https://www.incibe.es/aprendeciberseguridad/spear-phishing%22%20%5Cl%20%22%3A~%3Atext%3DEl%20spear%20phishing%20consiste%20en%2Cinformaci%C3%B3n%20confidencial%20de%20la%20v%C3%ADctima.), [spoofing](https://es.wikipedia.org/wiki/Suplantaci%C3%B3n) … en definitiva, ataques de [Ingeniería Social](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29). En el siguiente enlace podéis encontrar otro de nuestros artículos, donde veréis las diferentes técnicas que siguen los ciberdelincuentes para [HACER PHISHING](https://ciberinseguro.com/como-hacer-phishing/).

Para ello, lo primero que debemos tener es un equipo sobre el que instalemos la herramienta [Set Toolkit](https://github.com/trustedsec/social-engineer-toolkit). Se puede instalar en Windows, como muchos tendréis, pero mi recomendación es que utilicéis alguna distribución Linux, que además ya contenga Set Toolkit instalado, como por ejemplo, [Kali Linux](https://www.kali.org/docs/introduction/download-official-kali-linux-images/). En mi caso, utilizaré esta distribución, para ir mostrándoos este ataque.

Bueno, llegamos aquí, el primer paso sería abrir la aplicación. Para ello, tan solo debemos escribir “settoolkit”. Es posible que nos solicite permisos de root, es algo normal.

Una vez abierta la herramienta, nos aparecerá un menú con diferentes alternativas. En este caso, deberemos seleccionar la primera opción “Social-Engeneering Attacks”. Para ello, escribimos “1”.



A continuación, nos aparecerá otro menú, donde deberemos elegir la segunda opción “Website Attack Vectors”. Para ello deberemos escribir “2”. Esto es así, porque vamos a realizar un tipo de ataque, clonando una web legítima, para simular que somos quien no somos en realizar. Es decir, vamos a realizar una clonado de una web para realizar un ataque de Spoofing.



Cuando nos aparezca en siguiente menú, deberemos seleccionar la tercera opción, es decir, “Credential Hardvester Attack Method”. Escribimos por tanto el “3”.



En el siguiente menú, deberemos escoger la opción de “Site Clonner”, ya que como hemos indicado, vamos a clonar un sitio web legítimo. Escribimos el “2”.



A continuación, nos va a preguntar acerca de la dirección IP pública que vamos a dar a nuestro sitio web clonado. Esto es para indicar al servicio web que va a levantar la aplicación Set Toolkit, que dirección publica en el propio servicio. De esta forma, todas las peticiones que vayan a esta IP, las redirigirá a nuestro sitio clonado. Pero recordar que si vamos a publicarlo a Internet, debemos indicar una IP pública. Si simplemente vais a realizar alguna prueba de concepto, con una IP privada lo podéis probar.



En el siguiente paso, nos pregunta que sitio web queremos clonar. Pues en este caso, debemos incluir la dirección URL de la red social que queremos clonar. Por ejemplo, “https://twitter.com”.

Tu publicidad aquí



El último paso que nos solicita es si estamos seguros de lo que estamos haciendo, ya sabéis. Pues simplemente tenemos que escribir “s”.



Justo en este momento, nuestro sitio web falso, ya estará creado. Para probarlo, bastará con abrir un navegador y escribir la dirección IP que hemos indicado durante el proceso de configuración.

Si la IP es privada, porque es una prueba de concepto, solo vosotros podréis acceder a este sitio web clonado.

Si lo que queréis es enviar este sitio web a una tercera persona, debéis utilizar una dirección IP pública, evidentemente.

Tan solo bastará crear un correo electrónico, por ejemplo, simulando que sois, en este caso Twitter. Indicando que ha habido un problema en la cuenta del usuario, o que debe acceder a su cuenta si no quiere tener un bloqueo definitivo, o algo así, pero incluyendo un link donde el usuario pueda hacer clic. Este link debe contener la dirección de nuestro sitio web falso. De eta forma, cuando el usuario acceda a nuestro sitio web, e introduzca sus credenciales, nosotros estaremos capturando todo lo que escriban, y habremos conseguido su nombre de usuario y contraseña. Tan solo debemos volver a nuestra consola con Set Toolkit abierto, y veremos cómo nos muestra en texto plano estas credenciales.



A partir de aquí, os dejo a vosotros ser originales y ver como podéis enviar el link. Ya sea por correo, por SMS, a través de las redes sociales o como prefiráis.

En el siguiente enlace podéis encontrar otro de nuestros artículos, donde veréis las diferentes técnicas que siguen los ciberdelincuentes para saber CÓMO HACER PHISHING.

Tu publicidad aquí

Existen otras herramientas como Set Toolkit, pero creo que es una de las mejores, más rápidas y fiables para realizar este tipo de ataques.

Si quieres que hablemos de otro tipo de herramientas, déjame un comentario y lo trabajaremos para mostraros otras opciones.

Por otra parte, si utilizas este método y tienes dudas, déjame un comentario e intentaré ayudarte a resolverlas. Y por supuesto, si ya lo has utilizado, o ya conocías este método, cuéntanos tu experiencia.