HACKEAR FACEBOOK EN 30 SEGUNDOS sin paga 2022

Esto no significa que quieras dar ideas ..... Es cierto que no es fácil hacerlo, pero en el caso de las vulnerabilidades, es útil conocerlas para poder prevenirlas, tomar medidas y solucionarlas cuanto antes. Sin embargo, en este caso se trata de una vulnerabilidad conocida en el protocolo SS7 desde hace muchos años.

Cómo Hackear Faccebook online

Cuando se trata de redes sociales, "hackear cuentas de Facebook" o "espiar cuentas de Facebook" son probablemente dos de las búsquedas más populares en Google. Sin duda, es una de esas desagradables sugerencias que los profesionales de la seguridad reciben a menudo para ver si vale la pena probarlas. Ciertamente, hay algunas técnicas probadas que se pueden utilizar para hackear una cuenta de Facebook. Forbes informa sobre una técnica que los investigadores de seguridad han explorado utilizando una vulnerabilidad no del todo nueva. Todo lo que necesitabas era el número de teléfono de la víctima.

Vimos una técnica similar en este episodio de Hackerworld, en el que el experto en ciberseguridad Rubén Martínez consiguió acceder a la cuenta de Facebook de una víctima utilizando el doble factor de autenticación de la red social (por supuesto, primero tuvo que conseguir el número de teléfono de la víctima a través de un hotspot WiFi malicioso, pero esa es otra historia) ..... Lee por qué no debes conectarte a una red WiFi abierta sólo por diversión). Para obtener la contraseña y acceder a la red social de la víctima, logró obtener un SMS de autenticación (una conocida autenticación de dos factores) a través de una app maliciosa que instaló porque la víctima se había conectado a un punto de acceso WiFi falso. No es fácil, pero es posible.

Uso del sistema de hackear facebook sin encuesta

Los puntos débiles de esta red no sólo permiten el acceso ilegal a las redes sociales, sino también la vigilancia de las

llamadas telefónicas o la interceptación de los mensajes de texto. En este caso, para empezar a espiar, solo conocer el número de teléfono de la víctima y algunos datos sobre su dispositivo.Esta demostración fue realizada por investigadores de Positive Technologies, a quienes también se les mostró cómo acceder a las cuentas de WhatsApp y Telegram, según revela Forbes.

A pesar de los nuevos métodos de codificación utilizados en la red telefónica, el sistema SS7 resultó ser vulnerable. Estas vulnerabilidades se conocen desde hace varios años, ya que fueron reveladas en 2014 por un equipo de investigadores de una empresa alemana de investigación de seguridad.

En el caso de Facebook, un atacante hace clic en la opción "Olvidé mi contraseña" de la red social. Cuando el atacante pide el número de teléfono o la dirección de correo electrónico asociada a la cuenta, proporciona el número de teléfono de la víctima.

A continuación, el atacante envía un mensaje de texto al ordenador o al teléfono móvil de la víctima con un código de verificación enviado por la red social, obteniendo así acceso a la cuenta de Facebook de la víctima. Los investigadores muestran el proceso en este vídeo.

Este tipo de vulnerabilidad afecta a todos los usuarios de la red social que tengan activada esta opción de autenticación en dos pasos. Esto es irónico, ya que se supone que esta opción aumenta la seguridad de las cuentas. Los investigadores han demostrado que, además de Facebook, esta vulnerabilidad puede ser explotada por casi todos los servicios que utilizan la doble autenticación por SMS, como Twitter y Gmail.

El problema es que los operadores no han sido capaces de solucionar esta vulnerabilidad a corto plazo, y no es un problema de Facebook u otros servicios, sino de la propia red de telecomunicaciones.

¿Qué debo hacer como usuario para evitar que hackeen mi cuenta?

Desde luego, no es una técnica fácil; este tipo de técnicas requiere un alto nivel de conocimientos técnicos y dinero. Mientras tanto, los usuarios pueden tomar precauciones: desactivar la autenticación de dos factores en los servicios en los que está activada, no asociar su número de teléfono a las redes sociales y a diversos servicios, y utilizar temporalmente el correo electrónico como método de recuperación de la contraseña. O utilizar un método de autenticación de dos factores en el que no sea necesario enviar mensajes SMS.