

EL TIMO DEL CONOCIDO CON CUENTA ROBADA



Proyecto P-45 "Audaz"



Buenas a todos ciber-navegantes. Hoy os traigo un timo que hace poco estuvo a punto de sufrir un familiar. En este caso lo recibió por la aplicación **Messenger de Facebook**, pero variantes del mismo timo ya los he visto por otras aplicaciones similares como *WhatsApp*, *Telegram*, o incluso mensajes directos en cualquier red social. Se trata del **timo a través de un conocido suplantado**.



¿En qué consiste este timo?

El timo consiste en que te escribe un contacto conocido diciéndote algo así como "*Madre mía, mira quién se ha muerto*" seguido de **un enlace de estos raros acortados**, normalmente muy pequeños y compuestos por letras y números sin sentido.

No te quedes solo con este caso, en realidad pueden mandarte cualquier mensaje que te alarme y llame mucho tu atención, con tal de que hagas clic. Ejemplos son: "Oh Dios, ¡no me puedo creer que seas el de la foto!", "¿Pero en serio eres tú el que sale en este video???", "¡Mira lo que dice este de ti!", etc. Cualquier tipo de trampa para que abras una supuesta foto, video o audio.



Figura 1. Un ejemplo de este timo. Date cuenta del enlace acortado y del uso de emoticonos para darle veracidad. No te olvides que encima te lo manda un conocido. Fuente: <https://www.elsiglodetorreon.com.mx/noticia/2021/eres-tu-el-del-video-usuarios-alertan-sobre-mensaje-en-facebook-messenger.html>

Este tipo de mensajes suelen ser **muy realistas**, y normalmente no suelen delatar que muchos de ellos son mensajes enviados automáticamente (**bots**) aunque, como en la siguiente imagen pueden delatarse si te envían el mismo mensaje seguidamente.



Figura 2. Un timo de esta clase que se delata a si mismo por dejar indicios claros de que está automatizado. No confíes en que tengas la suerte de que te ocurra esto, normalmente no es así. Fuente: <https://elcorreoeb.es/extra/no-abras-el-mensaje-del-video-en-messenger-HX7462559>

Otra variante de estos timos suele **usar una imagen que simula que el sitio web** es legítimo, pero es solo eso, una imagen que te hace creer que el video es de YouTube cuando no es así (ni siquiera era un video!)

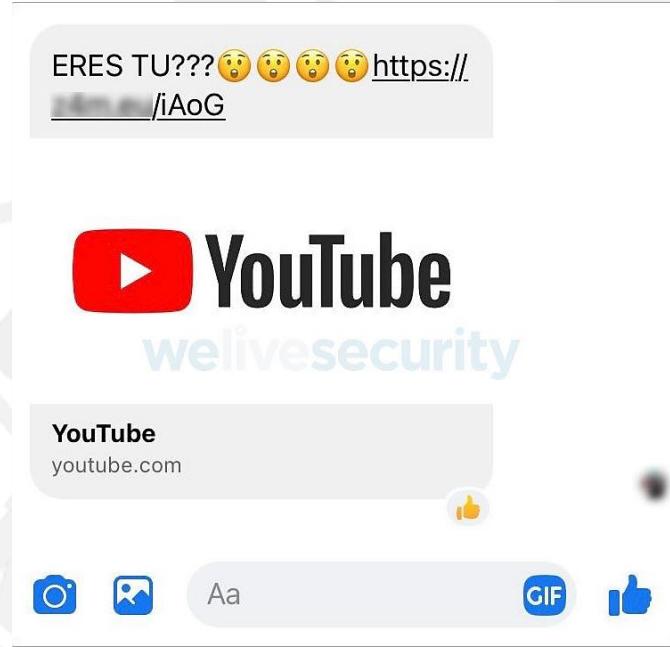


Figura 3. Mira cómo se usa una falsa imagen de YouTube para darle más credibilidad. Pero no es más que una imagen unida a un mensaje que lleva un enlace a un sitio malicioso. Fuente: <https://www.welivesecurity.com/la-es/2021/07/22/eres-tu-este-video-phishing-en-facebook-messenger/>

Date cuenta de que ninguno de estos mensajes se aprovecha de información que el delincuente puede tener por el hecho de que te lo está enviando un conocido. Esto es debido a que muchas veces están excesivamente automatizados para atacar al mayor nº de víctimas con el mínimo esfuerzo posible. Tampoco debes confiar en esto, porque si que hay muchos casos donde se usa lo que el atacante sabe sobre ti por estar usurpando la identidad de uno de tus contactos. Mira la siguiente imagen, por ejemplo. Aquí no solo **se usa el nombre de la víctima** (que el delincuente sabe por poder acceder a los contactos del suplantado) sino que la imagen que simula ser un video aparece borrosa y da toda la impresión de ser un video realmente privado.

En este caso se encuentra guardado en un servicio de almacenamiento de Google, que cualquiera puede contratar para guardar lo que sea.



Figura 4. Esta variante del timo usa el nombre de la víctima para ganar credibilidad. Fuente: <https://boliviaverifica.bo/recibiste-un-mensaje-con-un-supuesto-video-tuyo-no-lo-abras-es-un-virus/>

Como la mayoría de los timos **el objetivo de los estafadores es que hagas clic** o pulses el ese enlace y que entres en una página web preparada para cometer algún tipo de estafa con alguna excusa, o **instalar algún programa** también con algún pretexto.

 **Por ejemplo descargarte una aplicación para ver la supuesta esquila o cualquier locura que os podáis imaginar.**

Muchas veces también te encuentras **publicidad engañosa** diciéndote que tienes un virus y que te descargas un antivirus que ellas te dan (que es un *malware*) etc.

¿Me puedes poner un ejemplo de un caso real?

Aunque al final de la sección anterior te comento un poco qué pasa si picas y haces clic, lo cierto es que todo se entiende mejor si te explico un posible caso completo para que entiendas la estrategia que siguen, Vamos a ello. Pongamos el caso de la última imagen, con Víctor. Imagínate que **alguien suplanta al mejor amigo de Víctor** y le llega exactamente ese mensaje por *Facebook Messenger*. Viendo quien es el que le envía el mensaje, Víctor inmediatamente le hace clic, pero no le sale ningún video. Sin embargo, a Víctor le pasan estas dos cosas:

- **Pierde el acceso a su cuenta** de Facebook
- Descubre que en su entorno le ha llegado el mismo mensaje **a un montón de gente**.

¿Cómo es posible? No, **Víctor no ha perdido su cuenta solo por hacer un simple clic**. Lo que ocurrió es que al hacer clic en el supuesto video, le apareció esta pantalla:



Figura 5. Facebook te pide volver a darte de alta para ver el video...;o no es Facebook? Fuente: <https://boliviaverifica.bo/recibiste-un-mensaje-con-un-supuesto-video-tuyo-no-lo-abras-es-un-virus/>

Esta pantalla es **idéntica a la pantalla de entrar en Facebook**, y da la impresión de que simplemente Facebook le está pidiendo a Víctor que vuelva a verificar su identidad para ver el video. **Pero no es así:** Es una página falsa que copia el aspecto de Facebook, **que engaña a Víctor** y con la cual, al introducir su nombre de usuario y contraseña acaba de “donárselas” sin saberlo. *¿Entiendes ahora como Víctor perdió su cuenta?*

🔍 **Además, ten en cuenta que este mismo esquema se puede repetir con otros servicios, aplicaciones de mensajería, etc. donde se dé el mismo tipo de timo. Esto es solo una muestra de cómo actúan. Y sí, copiar el aspecto de una web es extremadamente fácil 😞**

Lo que pasa luego te lo puedes imaginar: con el usuario y contraseña de Víctor se hacen con su cuenta y todos sus datos, cambian la **contraseña** e impiden que el propietario legítimo pueda acceder a la misma (aunque **a veces no**, y permanecen “en silencio”). Finalmente, envía de forma automática el mismo tipo de engaño a todos los contactos de la víctima, repitiendo el proceso.

🔍 **¿Te das cuenta de como se propagan esta clase de estafas? Ahora entiendes porque pueden afectar a tanta gente: cada cuenta robada permite extender el problema más y más...**

¿Por qué un enlace acortado?

El motivo de usar enlaces acortados es para que **no puedas distinguir claramente a dónde apunta el mismo**. Mirad, los enlaces acortados son un servicio que ofrecen muchas páginas web para poder usar enlaces más pequeños para navegar a sitios. Es muy frecuente que cuando uno navegue a un sitio web le salga un enlace enorme, con parámetros, rutas, etc. que es difícil de recordar y de enviar por aplicaciones de mensajería o redes sociales que tengan un límite de caracteres. Aquí entran en juego estos enlaces.

Lo que hacen estos servicios es sencillo: tú pones una dirección de una página web y el servicio de crear enlaces acortados que uses te crea un enlace acortado que dirige a ese servicio (en la

imagen por ejemplo se está usando el servicio **anon.to**). Cuando alguien haga clic en ese enlace acortado, **anon.to** mira entre todos los que tiene guardados y te redirige automáticamente al sitio web real registrado como asociado al mismo, sin que tengas que hacer nada más. ¿Fácil, eh?

The screenshot shows the Anon.to website interface. At the top, there are navigation links for 'Anon.to' and 'Report', and on the right, 'Login' and 'Register'. Below the header, the title 'Anonymous URL Shortener' is displayed. A descriptive text says 'Create a secure anonymous short link from your url which also hides http referer!'. A text input field contains the URL 'https://www.redeszone.net/tutoriales/seuridad/evitar-datos-personales-dark-web/'. To the right of this field is a grey button labeled 'Shorten' with a red arrow pointing to it. Below the input field, the generated 'Short URL' is shown as 'https://anon.to/8D4Pzi' in a green box, followed by a green checkmark icon.

Figura 6. Servicio para acortar enlaces anon.to. Fuente: <https://www.redeszone.net/tutoriales/seuridad/direccion-url-real-enlaces-acortados/>

Todo esto está muy bien, pero el problema es que **no vemos a donde dirige una dirección realmente**. Por ejemplo, en la figura anterior no hay ningún indicio de que la página vaya a **redeszone.net**. Pues ahora imagínate a dónde te pueden llevar estos enlaces que te envían si les haces clic....

Por cierto, es importante que sepas que también hay servicios que **te dejan ver a dónde lleva un enlace acortado si se lo pones**, como el <https://unshorten.it/>, de la siguiente imagen:

The screenshot shows the Unshorten.it website. The main heading is 'Unshorten.It!'. At the top, there is a search bar with the URL 'https://anon.to/8D4Pzi' and a blue button labeled 'Unshorten.it!'. Below the search bar, a notice states: 'Notice: Woops! We can't seem to unshorten that URL, this could be for a few reasons, it may not be a short URL in the first place, it may not be a real URL or could no longer be active or the service used to shorten the URL may not be compatible with Unshorten.it!'. Another note says: 'Note that due to technical limitations, we do not support URL shortening services that do not take you directly to the destination website such as adf.ly which shows an advert before taking you to the final destination.' A green box below these notes contains the text: 'Below are the safety ratings for anon.to'. On the left, there is a section for 'Redirecting to https://www.redeszone.net/' with fields for 'Destination URL:' (containing 'https://anon.to/8D4Pzi') and 'Description:' (containing 'This site does not have a description available.'). On the right, there is a 'Screenshot Loading, please wait...' message with a small loading icon. Below this, there is a note: 'Screenshots for popular websites will load quicker than those of less popular sites.' Further down, there are sections for 'Safety Ratings (Provided by Web of Trust):', 'Trustworthiness:' (with a rating icon showing 0/5), 'Child Safety:' (with a rating icon showing 0/5), and 'Blacklists:' (listing 'hpHosts - Service Unavailable'). At the bottom, there are buttons for 'View Web of Trust Scorecard' and 'Go to https://anon.to/8D4Pzi'.

 **No obstante, esto te lo digo para que lo sepas. En este artículo **no nos vamos a fiar de NADA** que venga con una URL acortada como esta, y lo vamos a descartar directamente, así que mirarlo tiene poco sentido 😊**

¿Por qué tu conocido recibió este mensaje?

En este caso cuando se investigó de dónde venía este intento de timo, porque la persona que lo enviaba era una persona real y conocida de la víctima, se descubrió que la **cuenta de Facebook de la persona que lo enviada había sido robada** y se estaba usando para propagar un *malware* entre todos sus contactos.

 **Al hacer clic en la "esquela" te pedía que te la descargas y la abrieses en Word para poder verla. Al abrir la "esquela", el Word te pedía que "Habilitases contenido" para ver el documento...con esto daban paso a lo que realmente era esto: un documento con malware 😞**

Es muy probable que la persona que envío el mensaje hubiera sido víctima del mismo *malware* que ahora mismo estaba propagando, porque uno de sus efectos seguramente es intervenir las cuentas en redes sociales, como vimos en la sección anterior.

¿Y qué hago con esto?

Como os decía, este tipo de estafas ya las he visto en otros programas de mensajería o redes sociales con excusas variopintas. Recuerda lo que decíamos antes de decir "*¡no me puedo creer lo que estás haciendo en esta foto!*" o "*¿de verdad eres tú la que está saliendo en este vídeo?*". Como veis, todos son variantes para **crearte alarma o susto**, que entres en el enlace y comience la fase de propagar la estafa.

Y como la persona que os escribe es un contacto que conoces, es bastante más fácil caer en el problema. El único consejo que os puedo dar es que con este tipo de mensajes de alarma **nunca hay que hacer clic**, aunque vengan de alguien muy muy conocido o un familiar, y, en caso de duda, **contacta con él o ella por un medio diferente** al que se usó para hacerte llegar el mensaje para confirmar que esto realmente no es un timo. Mi familiar fue (felizmente) lo que hizo y por eso no cayó víctima de él.

Y si ahora mismo estás pensando "*no te puedes fiar ni de tu sombra en las redes*", lamento decirte que **tienes toda la razón**. Y como también te digo todas las semanas, no olvides comentarle estas cosas a todos tus conocidos y allegados para evitar que se lleven un disgusto, porque este tipo de cosas aparte de muy comunes pueden llegar a ser bastante dañinas. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, aunque conozcas a quien te escriba una petición extraña sigue siendo una petición extraña, ¡y más si te dice de hacer clic en algún sitio!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



1

- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en mi canal de YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [Si un contacto te envía este mensaje por Facebook Messenger, no lo abras \(02/04/2022\):](#)
- ['¿Eres tú el del video?', usuarios alertan sobre mensaje en Facebook Messenger \(05/07/2021\).](#)
- [No abras el mensaje del vídeo en Messenger \(07/09/2021\).](#)
- [¿Eres tú en este video? Campaña de phishing a través de Facebook Messenger \(22/07/2021\).](#)
- [¿Recibiste un mensaje con un supuesto video tuyo? No lo abras es un virus \(08/10/2021\).](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 06/03/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat