SÁQUELE MÁS JUGO A SU BIO EN INSTAGRAM | CÓMO ENFRENTAR UNA ENTREVISTA DE TRABAJO | LOS MEJORES JUEGOS RETRO DEL 2021

ENTER.CO

Viejas técnicas, nuevas trampas

Los mensajes extorsivos que le llegan desde su propio correo y el hackeo de WhatsApp se están volviendo comunes. Usan técnicas antiguas, pero con nuevos engaños. Cómo protegerse.

Edición 256

ISSN 2215-9134

Por Javier Méndez
Twitter: @javiermendezz

Fotos: Freepik Premium

Viejas técnicas nuevas trampas

Los delincuentes nos tienen asoleados estos días con variantes recientes de técnicas de engaño antiguas. Y se han vuelto más creativos, al punto que a veces nos hacen dudar. Cómo funcionan algunas trampas que son frecuentes estos días y cómo evitar caer.

A finales del 2020, una amiga me llamó para pedirme que hablara con su hija de 17 años, Luna, quien estaba muy preocupada por un mensaje que acababa de encontrar en su correo. Ese mail decía que habían tomado el control de su portátil. Además, aseguraban que tenían acceso a sus contactos, que controlaban la cámara y el micrófono, y que hacía varios días estaban grabando todo lo que ella hacía o decía. Le pedían una cifra en bitcoins para dejarla en paz, y le daban 48 horas de plazo para pagar.

Aunque al correo llegan constantemente mensajes extraños, y uno no les pone atención, un detalle de este le hizo pensar que la amenaza podía ser cierta: el mensaje le había llegado desde su dirección de correo del colegio. Es decir, el remitente era ella misma, así que parecía como si de verdad alguien controlara su computador, o al menos su cuenta de correo.

Después de contarle que el bitcoin estaba a casi 30 mil dólares, así que igual no podría pagarle al delincuente que la estaba acosando (el chiste no le hizo gracia), le expliqué que existía

una técnica que permitía falsear los remitentes de los correos, le pregunté si tenía antivirus en su computador (sí tenía) y le sugerí que borrara el mensaje y no se preocupara más por eso.

Su mamá me contó después que Luna no había quedado del todo tranquila, y eso me hizo pensar que debía escribir este artículo, además porque ese no era el primer incidente de seguridad informática que gente conocida me había mencionado en esos días. En ese y otros casos, aunque los delincuentes estaban usando técnicas que no son nuevas, como el spoofing o la ingeniería social, los engaños eran menos conocidos, y por eso podían ser más efectivos.

Por ejemplo, por la misma época, un periodista con el que trabajé hace unos años me envió un mensaje por WhatsApp avisándome que estaban usando su cuenta en esa app de manera fraudulenta. No se equivocaba. Apenas 30 minutos antes me había llegado por WhatsApp otro mensaje, que en teoría también era de él y que tenía su foto en el chat (aunque desde otro número que yo no conocía), en donde el impostor me decía que estaba organizando sus contactos de WhatsApp y me pedía que le confirmara si yo todavía tenía el mismo número de teléfono. El embaucador tenía acceso a los contactos del periodista, porque me saludó por mi nombre.

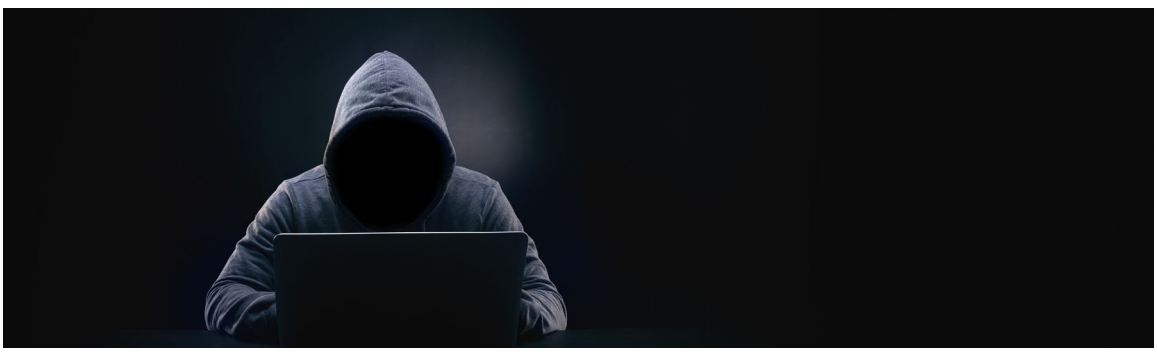
Cuando le contesté al remitente falso que sí seguía siendo mi número de teléfono, me envió un saludo de feliz año y no dijo nada más. No me extrañaría que un día de estos me contactara por chat para venderme algo o para proponerme algún negocio, pues eso es lo que hacen con esta nueva modalidad de fraude por WhatsApp, que se está volviendo común en Colombia.

El tercer incidente es mío, y es más común (phishing), pero alcanzó a preocuparme por el remitente: fue un correo de la DIAN en el que me avisaban que iban a embargar una de mis cuentas porque tenía un problema con mi declaración de renta.

La DIAN es algo así como el 'coco' para los adultos, así que yo le paro bolas a todo lo que me llega de esa entidad (y comienzo a hiperventilar y a sudar, como haría un niño ante la visión del 'coco'). Y me pareció extraño que el filtro de Outlook no mandara este mensaje a la carpeta de spam ni lo marcara como sospechoso, como suele suceder con ese tipo de correos (aunque últimamente el filtro de Outlook me deja entrar al buzón principal mensajes que es claro que son de phishing, y en cambio me filtra muchos que sí son legítimos; en Gmail también sucede, pero con menos frecuencia).

El caso es que abrí el supuesto mensaje de la DIAN, pero cuando vi que me invitaba a dar clic en un enlace para solucionar el problema, cerré el correo, no solo porque se veía sospechoso, sino porque no tenía mi nombre en el cuerpo del mensaje (usaba el genérico "estimado contribuyente") ni tampoco el número de mi cuenta, lo cual me daba pistas de que era un correo masivo que ni siquiera estaba personalizado (igual, a veces personalizan el phishing). Lo que hice después fue entrar por mi cuenta al sitio web de la DIAN (sin usar el enlace del correo) y todo estaba en orden.

Aunque pareciera que estos temas de seguridad informática están 'chuleados', y que ya no deberíamos caer en esas trampas, es evidente que los delincuentes se han vuelto más creativos y están usando trampas nuevas que por momentos nos pueden hacer dudar. Por eso, a continuación explico con más detalle cómo funcionan estos engaños desde el punto de vista técnico y qué medidas se pueden tomar para evitar ser víctima de ellos.



Por qué le llega un correo desde su propia cuenta

Que a uno le llegue un mensaje desde su propia cuenta es intimidante porque da a entender que alguien podría haber tomado el control del computador, pero esa es una técnica antigua llamada spoofing, que consiste en falsear una dirección de correo electrónico para que parezca que proviene de otro remitente. No es mucho lo que se puede hacer contra ese mal porque es sencillo falsear el remitente, pero los principales servicios de correo suelen marcar esos mensajes como sospechosos.

El remitente de los mensajes se puede falsear con facilidad a través de servicios para hackeo que están disponibles en Internet. Y los delincuentes usan esa técnica precisamente porque puede generar temor en las personas que reciben los mensajes.

Un artículo publicado en el blog de la empresa de seguridad informática Sophos explica que los delincuentes suelen decir en esos mensajes que han introducido en el equipo de la víctima un 'troyano' (una modalidad de virus) que les permite controlar el computador, la cámara y el micrófono, y que están grabando todo lo que la persona hace.

También suelen amenazar a la persona con enviar un video que han capturado a todos sus contactos, o a sus seguidores en redes sociales, a menos que se pague una cantidad en bitcoins. En algunos casos incluyen en el mensaje una o más contraseñas que la persona conoce (generalmente antiguas), como una prueba de que controlan el computador

(esas contraseñas las sacan de bases de datos de contraseñas robadas que se venden en lugares como la Dark Web).

Con todos esos datos en un correo que encima viene desde la dirección de uno mismo, es entendible que la persona se preocupe y crea que realmente controlan su computador. "La buena noticia es que eso no es cierto", dice la empresa Sophos, que agrega: "El delincuente no ha demostrado que haya hackeado su correo electrónico. Todo lo que ha demostrado es que cualquiera puede enviar un correo que parece ser de otro remitente".

Sophos explica que el spoofing no es una técnica nueva, y que esta variante apela a los temores de la gente, ya que técnicamente sí es posible hackear la cámara o el micrófono, por lo que algunas personas terminan pagando la cifra que se les pide. También puede pasar que la dirección se falsee no para que parezca venir de su propia cuenta de correo, sino la de un amigo o familiar suyo, así que usted también debería ser cauto con los mensajes sospechosos que le lleguen de personas conocidas. Pueden ser falsos.

¿Cómo sabe que lo están engañando?

La forma más fácil es que uno revise la carpeta de mensajes enviados de su correo. Con toda seguridad, el mensaje intimidante que supuestamente salió de nuestro correo no estará allí.

También es bastante probable que el mensaje ni siquiera llegue al buzón principal, sino que sea enviado por servicios de correo como Gmail y Outlook a la carpeta de spam; además, estará marcado como 'sospechoso' cuando uno lo abre. El problema es que los filtros de correo están llenos de falsos positivos: marcan como si fuera spam tanto mensaje legítimo que ahora uno tiene que andar revisando la carpeta de correo no deseado constantemente.

Por ejemplo, cuando hablé de nuevo con Luna, me confirmó que era en esa carpeta en donde había encontrado el mensaje intimidatorio. Ella estaba revisando la carpeta de spam porque quería verificar si la universidad para la que está aplicando le había contestado. Y, en efecto, allí estaba refundido un mensaje legítimo de la universidad; los filtros de correo, insisto, están filtrando demasiados mensajes que son confiables (les pasa con nuestros mensajes a muchos suscriptores de la revista, especialmente los que tienen cuentas de Outlook).

Por qué pueden tener contraseñas suyas

¿Que le manden una contraseña suya (algo que a veces pasa con los mensajes que falsean el remitente) no quiere decir que de verdad han penetrado en su PC?

No. Lo que sucede es que con cierta frecuencia se producen robos masivos de contraseñas en los sitios de empresas y en servicios web de todo tipo. Por ejemplo, Adobe, LinkedIn y Dropbox han sido víctimas de esas fugas de datos. Generalmente, lo que sustraen es la contraseña y el correo electrónico de los usuarios del servicio vulnerado. Y esos datos de millones de usuarios los delincuentes los compran y los venden en la Dark Web, una zona de Internet a la que no se tiene acceso desde un navegador convencional, y en donde se realizan todo tipo de transacciones ilegales.

Por eso es tan importante tener contraseñas diferentes para cada servicio web que uno usa. Si usted emplea la misma clave en todos lados, y encima no la cambia nunca, un delincuente tendrá acceso a todos sus servicios

y cuentas de Internet comprando esas bases de datos.

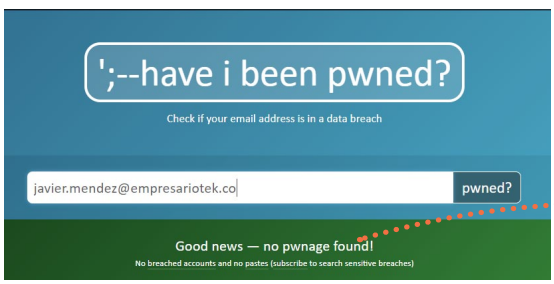
Por ejemplo, en el 2016 fueron hackeadas las cuentas en redes sociales de varias celebridades, entre ellas la cantante Katy Perry, que temporalmente perdió el control de una cuenta de Twitter que en ese momento tenía 90 millones de seguidores. Mark Zuckerberg, el fundador y presidente de Facebook, y un experto en tecnología, fue otra de las víctimas: no penetraron en su cuenta de Facebook, pero sí tomaron el control de cuentas suyas en Twitter, Instagram y Pinterest.

Después se supo que los delincuentes que hackearon a esas y otras celebridades en realidad no habían vulnerado ni la seguridad de Twitter, ni la de Facebook. Las contraseñas con las que tomaron el control de esas cuentas las habían encontrado en una base de datos que le habían robado cuatro años antes a LinkedIn, con los datos de 177 millones de sus usuarios, y la cual estaba disponible en la Dark Web.

Teniendo los datos de acceso a LinkedIn de esas personas, los delincuentes pudieron entrar en otras cuentas y redes sociales porque Mark Zuckerberg, Katy Perry y las otras víctimas habían cometido el error de emplear el mismo correo electrónico y la misma contraseña como usuario y password de varios de los servicios que usaban en Internet.

Ahora bien, ¿cómo sabe usted si algunas contraseñas suyas han sido robadas y están disponibles públicamente en Internet junto con su correo electrónico? Visite el sitio Have I Been Pwned? (haveibeenpwned.com) e introduzca su dirección de correo electrónico. Es altamente probable que este sitio le diga que ese correo, y la contraseña con la que lo usó como usuario en algunos servicios, está disponible en bases de datos que fueron robadas (verá la palabra "pwned", que es un slang para 'derrotado'). Además, el sitio le informará cuáles fueron los servicios web vulnerados en donde se robaron esos datos suyos.

Por ejemplo, aquí muestra que mi dirección de correo javier.mendez@enter.co (el usuario de algunas de mis cuentas en Internet), junto con las contraseñas que usaba hace unos años en Dropbox, en un servicio de Adobe y en LinkedIn, aparecen en algunas de esas bases de datos.



Si sus datos no aparecen en bases de datos robadas, el mensaje que verá es este.

Eso no me preocupa porque, aunque es dispendioso, yo uso una contraseña diferente para cada servicio web, y las cambio con regularidad. Además, tengo una buena cantidad de cuentas de correo diferentes para dispersar el riesgo. Y mis direcciones de correo personales, las que uso como usuario en los servicios más importantes, no las menciono en ningún sitio público, ni se las doy a nadie (explico cómo crear contraseñas seguras en esta nota publicada hace unos años en ENTER.CO: bit.ly/39cuKsE).

Pero realmente lo que me permite estar más tranquilo es otra cosa: yo uso la autenticación de dos pasos en todos los servicios que la permiten. Esa es una medida de protección clave, que usted debería adoptar, porque así nadie más podrá acceder a sus servicios de Internet, así tengan su contraseña. La razón es que el delincuente también necesitará acceso a su celular para recibir un código de verificación (bueno, a veces hacen algo llamado hackeo de SIM para 'adueñarse' de su celular, pero no lo voy a estresar con eso aquí; hay una nota sobre ese tema en este enlace: bit.ly/3qIl0kz).

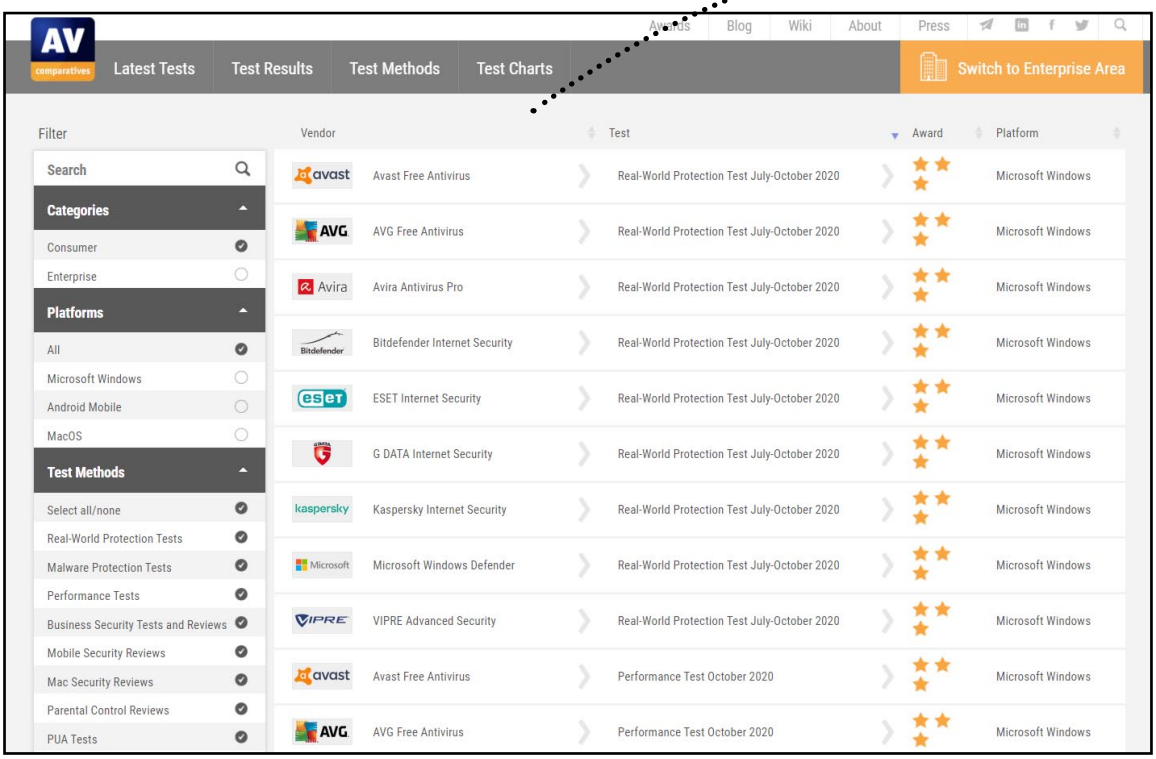
Un consejo final sobre la autenticación de dos pasos: a veces, los SMS con los códigos de verificación de la autenticación de dos pasos no llegan al celular, o se demoran demasiado. Por eso, es preferible que use una app de autenticación para generarlos en su teléfono; las apps más conocidas son Microsoft Authenticator y Google Authenticator.

Lo mejor es que esas apps ahora funcionan con muchos servicios de otras empresas; por ejemplo, Amazon, MailChimp y algunos servicios de hosting aceptan los códigos de Google Authenticator (en la edición 216 de ENTER se explica cómo funciona la autenticación de dos pasos y cómo usarla con esas apps).

¿Qué peligros sí son reales?

Queda claro entonces que esos mensajes con remitentes falsos no deberían preocuparle. Pero lo que sí es real es que se pueden hackear las cámaras y los micrófonos de los computadores a través de malware.

En ese caso, la primera línea de defensa es un buen antivirus, es decir, los que suelen encabezar las listas que publican entidades independientes de pruebas, como los laboratorios europeos AV Comparatives (www.av-comparatives.org) y AV Test (www.av-test.org).



Algunos de ellos son Kaspersky, Avast, Bitdefender y AVG. Y una buena noticia es que Windows Defender ha empezado a salir bien ubicado en esas pruebas (es el antivirus de Microsoft que viene incorporado en Windows 10). Además, usted debe estar pendiente de mantener su antivirus actualizado.

La otra protección es no dar clic en los archivos sospechosos que le lleguen por correo. Y todos los archivos que baje de Internet, o los que sus conocidos le manden por correo o por WhatsApp, debería revisarlos siempre con el antivirus, así parezcan confiables (sus conocidos podrían no tener antivirus en sus computadores).

Si quiere estar aún más tranquilo, usted podría poner un pedazo de cinta aislante o de cinta masking sobre la cámara de su portátil cuando no la esté empleando. Incluso, ahora hay portátiles que tienen una pestaña que permite mantener la cámara tapada cuando no está en uso.

El ransomware también es una amenaza

Finalmente, sobre el tema de mensajes en donde lo extorsionan para que pague una cifra en bitcoins, es importante mencionar que sí es muy real la amenaza del ransomware.

Este es un tipo de ataque en el que introducen en el computador de la víctima un malware que toma el control de la máquina y encripta todo su contenido hasta que la persona pague un rescate en bitcoins.

El ransomware es un tipo de malware, así que se distribuye muy fácilmente y de forma masiva por Internet y por correo, pero lo bueno es que, como es un tipo de virus, los antivirus también lo atajan. Pero la precaución más importante que puede tomar en el caso del ransomware, por si alguna vez llega a ser víctima de él, es mantener siempre copias de seguridad recientes en una unidad de almacenamiento externa (que esté guardada, no conectada todo el tiempo en su computador, porque el ransomware también encripta los discos externos).

Para que tenga una referencia de a qué me refiero con "recientes", yo saco una copia de seguridad diaria de algunos archivos que son muy relevantes para mí. Suena tedioso, pero es simplemente un hábito que me quita pocos segundos al día. Además, hago un backup completo de las carpetas importantes de mi computador cada 15 días. De esa forma, si tengo algún incidente de seguridad, me puedo recuperar sin que sea tan traumático.

Cómo pueden hackear su cuenta de WhatsApp

El caso del periodista que mencioné al comienzo de este artículo, cuyo WhatsApp fue hackeado, infortunadamente no es un hecho aislado. En los últimos meses se han presentado varios incidentes similares en el país, que han sido reportados por los medios de comunicación.

En este tipo de hackeo se recurre a la ingeniería social para convencer a una persona de que le mande a un conocido un código que le ha llegado a su celular en un mensaje de SMS. Por ejemplo, suponga que usted recibe de su hermana un mensaje que le dice: "Javier, cambié de celular y de número de teléfono; este es el nuevo para que lo guarde. Y necesito un favor: estoy terminando de configurar WhatsApp en el celular nuevo y no me están funcionando los SMS, así que necesito urgente un código de verificación que le hice enviar a su teléfono para poder terminar de configurar WhatsApp porque a ratos se me está bloqueando".

¿Suena razonable? Una persona confiada podría pensar que no hay nada de raro en eso, más sí ve en el chat desde donde le llega ese mensaje la foto de su hermana (el mensaje falso que me llegó de mi colega periodista incluía en el chat la misma foto que él tiene en el chat real, solo que desde un número de teléfono diferente). Por eso, alguien podría caer en la trampa y enviar ese código de verificación, sin saber que en realidad le está enviando a un delincuente el código que WhatsApp le manda a uno cuando cambia de teléfono.

Es decir, lo que el impostor está haciendo es instalar la cuenta de WhatsApp de la víctima en un celular nuevo, y como para ello ese servicio le envía un código de verificación al celular de la víctima, el impostor simplemente se lo pide haciéndole creer que se trata de otra cosa. ¿Y cómo sabe el delincuente cuál es su número o quién es su hermana? Una forma es porque algunas personas tienen esos datos públicamente en sus redes sociales. Y otra manera es porque, antes de mandarle ese mensaje a usted, ya hackearon a un conocido suyo con la misma técnica.

Se lo explico de otra forma, pero no yendo hacia atrás, sino hacia adelante: si usted cae en la trampa con el mensaje de su

hermana, se apoderan de su cuenta de WhatsApp, tienen acceso a sus contactos, y el delincuente repite el mismo procedimiento con ellos: es decir, les pide un código de verificación que le permite acceder a sus cuentas de WhatsApp. Y así repite el proceso con aquellos que cayeron en el engaño. Es una especie de pirámide en la que cada vez tienen más contactos para atacar.

Otra forma como a veces tratan de sonsacar esos códigos de verificación es enviándole a la persona un mensaje que dice algo como: "Somos del departamento de seguridad de WhatsApp, y hemos detectado que su cuenta se activó en otro equipo. Como medida de seguridad le hemos enviado un SMS para confirmar que la nueva instalación sea legítima; por favor, envíenos ese código".

Estos hackeos se aprovechan de que uno puede instalar su cuenta de WhatsApp en un celular sin SIM (todo lo que necesita es introducir el número de teléfono de la cuenta), siempre y cuando la SIM esté en el teléfono que recibe el código de verificación (WhatsApp también permite que uno cambie de número de teléfono y migre el contenido de su cuenta anterior al número nuevo). Así que los delincuentes no necesitan la SIM de su celular, sino ese código de verificación que le sonsacan.

¿Y qué hacen los delincuentes con esos contactos que engañan? Pedirles dinero. Por ejemplo, el impostor podría escribirle a una persona haciéndose pasar por un familiar para decirle que tiene un problema grave y necesita que le consigne urgentemente un dinero para salir ese mismo día del lío. En últimas, las víctimas terminan siendo los contactos, y no la persona a quien originalmente le hackearon la cuenta de WhatsApp, lo cual tiene un riesgo de reputación grande para uno.

Algunos de los que han caído en las trampas reportadas por los medios de comunicación les enviaron plata a los impostores porque estos les hicieron creer que tenían una oportunidad única de comprar dólares a una tasa de cambio muy favorable. Lo sorprendente es que haya gente que hace ese tipo de transacciones sin tomarse la molestia de llamar por teléfono a su supuesto amigo o conocido. Les basta un simple chat. Imagino que precisamente por ser tan confiados caen en esas trampas.

Cómo evita uno esos engaños

Obviamente, la forma de protegerse de esta trampa es meterse en la cabeza que uno jamás le debe enviar a otra persona los códigos de verificación que le llegan a su celular. Pero hay una solución más permanente: WhatsApp tiene una autenticación de dos pasos, que vale la pena activar inmediatamente.

Se trata de un PIN de seis dígitos que no cambia (es como una especie de contraseña), el cual le pedirán siempre que su cuenta se trate de activar en otro teléfono. Ese PIN es adicional al código que le mandan por SMS; por eso, así un delincuente lo convenciera de enviarle el código del SMS, no podría activar su cuenta porque necesitaría el otro número.

El PIN de la autenticación de dos pasos lo debe tener siempre presente porque, una vez se activa, WhatsApp lo pide de vez en cuando así no se esté cambiando de teléfono (supongo que como medida de seguridad). Se activa de la siguiente forma:

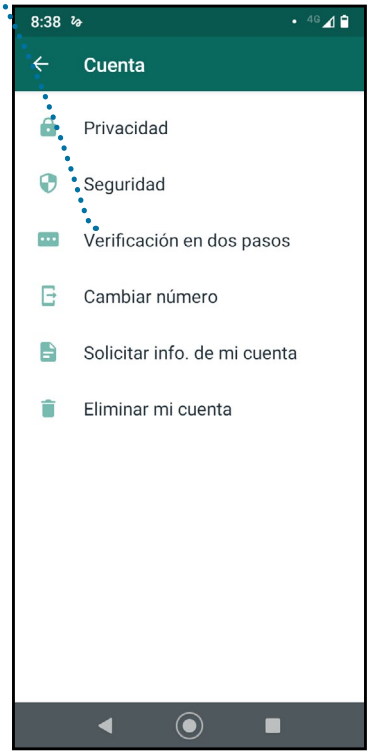
Abra WhatsApp, en Android toque los puntos suspensivos que hay arriba a la derecha (en iOS

toque el botón Configuración abajo), seleccione Ajustes, luego la opción Cuenta y toque en 'Verificación de dos pasos'.

Ahora toque el botón Activar, escriba el PIN (es un número de seis dígitos) y agregue una dirección de correo electrónico; el mail es opcional, pero es útil porque le permitirá recuperar su cuenta si llega a olvidar el PIN.

Eso es todo. En adelante, al cambiar su cuenta de WhatsApp a otro teléfono, deberá introducir ese PIN después de haber escrito el código de verificación que le mandan por SMS.

Lo otro que debe saber es que, cuando el delincuente toma el control de su cuenta de WhatsApp, a usted lo sacan de la suya en su celular. Pero si usted trata de configurarla de nuevo, como si estuviera instalando la app en un teléfono nuevo, el impostor queda desconectado; usted simplemente pide otro código de verificación y entra de nuevo. El impostor juega entonces con la posibilidad de que pase un tiempo largo antes de que usted note que algo está mal con su WhatsApp, y que además usted se demore en restablecer su cuenta.



Pero hay un riesgo adicional si no tiene activada la verificación de dos pasos: si usted no ha tomado esa medida, que es la única que evita este tipo de hackeos, corre el riesgo de que sea el delincuente el que active el PIN en su cuenta, y entonces usted ya no podría recuperar su cuenta durante siete días porque no sabría cuál es el PIN que puso el impostor.

WhatsApp explica en su sitio web (bit.ly/3qHOqKC) que después de esos siete días usted podrá volver a entrar a su cuenta sin el PIN, y además el impostor quedará fuera de su cuenta desde el momento en que usted introduce el código de verificación que llega por SMS. Pero definitivamente es mejor activar el PIN usted mismo y así se evita todos estos riesgos.

¿Y sobre el phishing?

Sobre el tercer caso del que hablé al comienzo del artículo –el mensaje falso de la DIAN– no hay mucho que decir en la parte técnica porque el phishing sigue funcionando como siempre: le llega un mensaje que lo invita a dar clic en un enlace que lo conduce a un sitio falso para que introduzca sus datos financieros u otro tipo de información. O también podría ser la forma como activan un malware en su equipo.

Pero mencioné ese episodio solo para dejarle la inquietud de que los engaños de esos mensajes cambian constantemente y a veces son cosas que pueden generar dudas, como ese falso mensaje de la DIAN. Antes eran correos de supuestas fotomultas, y uno pensaba que el archivo anexo traía la foto que mostraba cuál había sido la infracción. En unos meses quizás sean correos que le dicen que el archivo anexo contiene los datos de su cita para ponerse la vacuna contra el covid-19.

Es fácil caer en esas trampas, pero es clave que dude de todos los mensajes no solicitados que le llegan. Y si queda con dudas,

lo que debe hacer es averiguar –sin dar clic en los enlaces– directamente con las entidades que supuestamente se están comunicando con usted.