¿Qué pasa si perdemos las claves del Google Authenticator?

¿Alguna vez usaron el Google Authenticator? Si la respuesta es positiva sabes de que estamos hablando. Para los que no lo conocen pasamos a explicar brevemente para poner a todo el mundo en contexto.

En la actualidad, es cada vez más común que las personas usen medios de pago alternativos al dinero FIAT *(Dinero Papel).* Esto es una tendencia mundial, ya que todos los bancos centrales de los países están tratando de eliminar de a poco los billetes tal como los conocemos para reemplazarlos por estos medios alternativos. Por este motivo en la última década, se incrementó en forma exponencial el uso de diferentes medios de pago. Algunos ya eran usados desde antes *(como por ej: tarjeta de Débito y de crédito),* pero no todo el mundo tenía acceso a estos medios. Hoy, sin embargo, hasta los jubilados y las personas que cobran planes o subsidios cuentan con una caja de ahorro y tarjeta de débito.

Los otros métodos son mas recientes y no todos aun los utilizan. De lo que estamos hablando es de los sistemas de pago electrónico, o también llamados "Billeteras Digitales" *(término utilizado por la mayoría en la actualidad).*

Nuevas tecnologías, nuevos problemas:

Todos estos avances tecnológicos en el sistema de Pagos brindan un montón de beneficios, los cuales no vamos a enumerar ya que no es el objetivo del artículo, pero también presentan varios inconvenientes; sobre todo si las personas que los usan no entienden bien el concepto ni los alcances de la tecnología que están usando.

A raíz de esta falta de conocimiento en mas de la mitad de los usuarios, se incrementó también la cantidad de estafas o robos virtuales, donde los usuarios perdían todo su dinero.

Para solucionar este inconveniente se empezaron a fortalecer las medidas de seguridad asociadas a cada plataforma. Generalmente todos usan los mismos métodos y básicamente consisten en la mayoría de estos ítems.

- **Políticas de Contraseñas mas robustas**, *donde se obliga el cliente a utilizar contraseñas mas largas (mínimo 8 caracteres), alfanuméricas (números y letras), mayúsculas y minúsculas y caracteres especiales (.,*-).*
- **Correo de recuperación**, *donde se envía un link a cada cliente para acceder a un portal donde se puede entre otras cosas, resetear el password o activar la cuenta.*
- **Preguntas de Seguridad**, *donde cada cliente puede elegir una serie de entre 3 y 5 preguntas básicas y debe escribir cada una de las respuestas (ej: nombre del colegio primario) que van a ser requeridas en caso de olvidar la contraseña o tener problemas en el ingreso.*
- **Mensaje de SMS al teléfono móvil**, *esta opción es la mas nueva de todas, y cada vez mas plataformas la usan no solo para resetear claves, sino que se emplea para ingresar a la aplicación en forma cotidiana (el cliente además de poner el usuario y la clave, debe esperar el código SMS en su celular e ingresarlo para recién poder acceder a los datos personales).*

Método de autenticación de 2 factores o vías:

Con el aumento del uso de plataformas de inversión y el boom de las criptomonedas muchos brokers o agentes de Bolsa *(entidades similares a bancos que permiten operar varios instrumentos como acciones, bonos, ETFs, etc.)* o Exchanges *(Plataforma similar a un bróker pero para criptomonedas que permite comprar, enviar e intercambiarlas entre usuarios)* decidieron dar un paso mas a nivel seguridad, y sumado a los métodos anteriormente mencionados agregaron uno adicional llamado "método de autenticación de 2 factores/vías" o 2FA/2WA por sus siglas en inglés *(Two Factor / Way Authentication).*

Este método consiste utilizar un algoritmo, que emparejado con la plataforma a utilizar, genera un código único aleatorio para cada usuario que caduca a los 30 segundos. Finalizado ese tiempo, el algoritmo genera un código nuevo. Debido a la corta duración del código este sistema, sumado a las otras medidas comentadas anteriormente, brinda un muy buen nivel de seguridad difícil de vulnerar *(aunque no imposible).*

En sus comienzos, esta tecnología utilizaba dispositivos de Hardware *(generalmente de la marca RSA)* que se podían agregar al llavero y mostraban los códigos hasta que se agotaba la batería. Ahí se debía gestionar un nuevo token. *(ver foto a continuación).*

En la actualizad muchas plataformas decidieron cambiar este método por aplicativos móviles que cumplen la misma función. Es aquí donde aparece por ej "**Google Authenticator**"o "**Microsoft Authenticator**" entre los mas conocidos o usados.

Otros aplicativos similares pueden ser:

- Aegis Authenticator
- 2FA Authenticator
- Authy

Habiendo realizado una breve introducción al tema, volvemos entonces a la pregunta que da título a este artículo.

¿Qué pasa si por algún motivo, sea este robo, perdida o rotura del móvil, perdemos acceso a los códigos generados por el Google Authenticator o aplicativo similar?

La respuesta es muy simple. ESTAMOS EN PROBLEMAS.

Hace menos de un mes me pasó exactamente eso, por lo que las próximas líneas van a ser una breve descripción de lo que sufrí para lograr hacer funcionar todo nuevamente, y un consejo simple de cómo evitar que les pasé a ustedes.

Mi experiencia:

Un día normal de semana por la tarde estaba en casa con mi Hijo Giovanni de 8 años, el cual tiene una energía enorme y por momentos se pone muy demandante, y necesitaba terminar un trabajo que me había comprometido a entregar ese día, por lo que se me ocurrió darle el teléfono móvil para que juegue o vea videos de Youtube un rato mientras yo podía usar la PC para continuar con mis compromisos.

Mientras yo avanzaba en mis tareas, no me di cuenta que Gio instaló algunos juegos, como suele hacer generalmente, pero esta vez como se quedó sin espacio, borró la aplicación Google Authenticator del móvil.

Para cuando me di cuenta ya estaba desinstalada, por lo que decidí explicarle que no puede borrar aplicaciones del teléfono, que no sean juegos, sin preguntar previamente y le dije que no se preocupe que lo instalaba nuevamente y se solucionaba el problema. Mi sorpresa fue grande cuando, luego de instalar nuevamente la app, ***estaba completamente en blanco***. Yo pensé "erróneamente" que al estar registrada con mi correo, al volverla a instalar iban a aparecer todos los códigos que tenia generados, que para ese momento eran aprox. 10. *(entre diferentes bancos, exchanges y billeteras varias)*.

Sin entrar en detalles muy técnicos para no aburrir y ser entendible para todos, nuevamente subestimé el problema al pensar que solamente iba a perder un poco de tiempo al generar todo nuevamente. Como imaginaran, no fue tan fácil. Lo que ocurrió, es que para generar un nuevo código, por ej de un Banco, primero tengo que ingresar a la App, o a la web del banco. Y para poder ingresar a la plataforma me pide como medida de seguridad el código, que justamente **acababa de perder**. Resumiendo… Tuve que mandar mails, o contactar por chat o diferentes formas de mensajería al soporte de cada aplicación *(recuerden que tenía aprox. 10)* y solicitar que me borren ese método de seguridad para que me deje ingresar solamente con usuario, clave y a lo sumo mensaje SMS.

Todos, los 10, demoraron varias horas en contestar y evaluar la solicitud y en ese lapso de tiempo me bloquearon el acceso a sus servicios hasta que estuvieran seguros que era un pedido licito y no se trataba de alguna estafa.

Como se imaginarán ***estuve varias horas completamente fuera del sistema***, sin acceso a mis inversiones, mis cuentas, dinero, etc. Lo único que podía hacer es pagar físicamente en un local con la tarjeta de débito o crédito, pero no me dejaba hacer transferencias electrónicas entre cuentas *(algo que suelo usar mucho para casi todo, incluso las compras).*

Recuerdo que al día siguiente estuve toda la mañana, hasta casi las 13 hs solamente para regularizar el acceso al homebanking *(página web de mi banco).* Me llevó otra cantidad de tiempo similar arreglar el acceso a uno de mis exchanges principales, por lo que se puede decir que en un día logré normalizar el acceso a 2 plataformas, algo que fue bueno y un alivio en su momento, pero aún me faltaba arreglar 8 más. ☹

Finalmente, después de casi 3 días pude regularizar la situación, pero fue un proceso bastante engorroso, ya que tuve que darme de baja en casi todos los sitios y volver a darme de alta, con todo lo que eso implica *(llenar formularios con muchos datos, enviar fotos de DNI, boleta de servicios, Selfies con DNI en mano, etc.).*

Mi consejo:

Para evitar todos estos inconvenientes hay que hacer un respaldo de la configuración del Authenticator para que al restaurarlo podamos contar con los códigos.

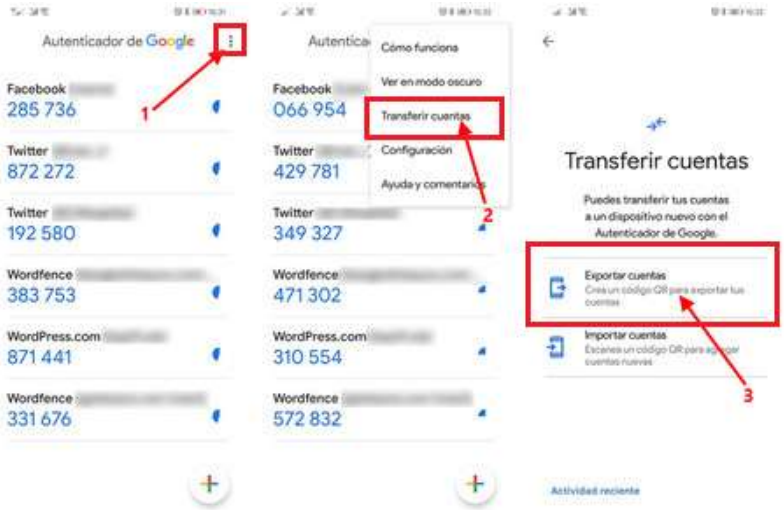
Hay varias formas de realizar un Backup de esta información, pero generalmente es algo no muy amigable para todo el mundo y muchas veces pueden llegar a necesitar asistencia de alguien que entienda un poco de tecnología y sobre todo de este tipo de aplicaciones de validación.

Si cuentan con esa ayuda, les comento que hay muchos instructivos en internet donde explican el paso a paso para cada aplicación por lo que detallarlo acá seria redundar información y hacer demasiado técnico el artículo.

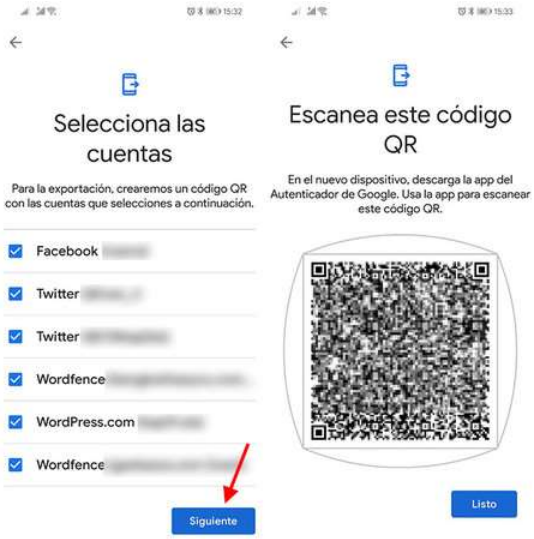
Como no todo el mundo tiene ese tipo de contactos, y el objetivo de este informe es poder ayudar a esas personas, permítanme indicarles una forma fácil que encontré para realizar el respaldo, aunque no sea la ideal o más correcta técnicamente hablando.

Para solucionar este inconveniente solamente hay que contar con ***dos teléfonos móviles*** (puede ser el de la pareja, hijos, etc.) y lo que tenemos que hacer es pasar los datos de nuestra cuenta al segundo móvil. De esta forma cuando tengamos algún inconveniente en el teléfono principal podemos acceder al de respaldo para migrar la cuenta al nuestro nuevamente.

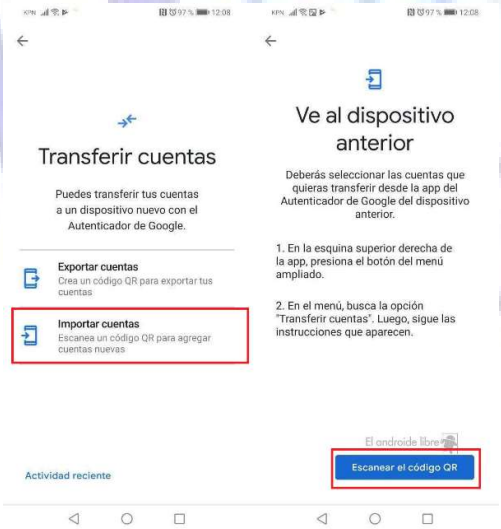
Esto se hace de la siguiente forma. Vamos al Google Authenticator y dentro de la aplicación vamos a los 3 puntitos *(1)*, seleccionamos la opción "***Transferir Cuentas***" *(2)* y luego "***Exportar Cuentas***" *(3).*



Luego de darle click a "***Exportar cuentas***" nos solicita marcar todas las cuentas a pasar. Ahí marcamos todas *(salvo alguna puntual que no queramos pasar)*, le damos a siguiente y ahí nos sale un código QR para escanear como se muestra en la siguiente figura.



Al obtener esto ***pasamos al segundo móvil***, ingresamos a la aplicación y repetimos el primer paso, solo que esta vez seleccionamos la opción "***Importar Cuentas***" y en la pantalla que nos sale seleccionamos "***Escanear el código QR***"



Escaneamos el código que nos muestra y listo. Ya están las cuentas en ambos teléfonos. Ya estamos respaldados por si ocurre algo con alguno de los móviles.