Verificación en dos pasos: ¿Garantía de seguridad o parche temporal?

Hace unos días, y tan sólo una semana después de presentar una nueva aplicación para iOS con nuevas opciones de búsqueda y capacidades para descubrir contenido de interés, **Tumblr** se veía obligada a lanzar una actualización de seguridad catalogada como "muy importante" y dirigida precisamente a los usuarios de teléfonos iPhone y tabletas iPad. No en vano, se había detectado un agujero que daba la bienvenida a potenciales ciberdelincuentes, permitiendo la vulneración de las credenciales de acceso a las cuentas de la red de microblogging "en determinadas circunstancias". Aunque la compañía, ahora propiedad de Yahoo!, no ha querido dar más detalles de lo sucedido y se ha limitado a recomendar la instalación del parche y la modificación de las contraseñas, hay quien asegura que el problema se encontraba en la falta de cifrado y el envío de los datos de inicio de sesión en texto plano a través de redes abiertas por un error de programación.

El peligro de una contraseña débil

El fallo ya ha sido subsanado, pero el peligro es evidente. **Las contraseñas se han convertido en un objeto de gran valor para terceros con malas intenciones** porque, más allá de otorgar libre acceso al mundo personal de la víctima, a sus secretos banales (o no tan banales) y a su identidad virtual, que no es poco, también pueden ser la llave que abra la puerta para desvalijar sus cuentas corrientes. El problema se acentúa cuando, bugs como éste aparte, los expertos coinciden en constatar una desidia general por parte de los propios interesados a la hora de seguir un manual de buenas prácticas.

Una de las equivocaciones más generalizadas es utilizar la misma secuencia de letras y números para todos los servicios online en los que se está registrado, ya que una vez descubierta la clave para uno de ellos es posible provocar la caída de todos los demás como si de fichas de dominó se tratase. También es un desacierto común utilizar palabras fáciles de adivinar, bien por tratarse de términos simplones y profusamente usados, por seguir el orden numérico lógico o por estar fuertemente vinculados a la vida de sus propietarios, esto es, por corresponderse con una fecha clave, el nombre de un pariente o ser el mero reflejo de sus gustos y aficiones. Eso por no hablar de quienes no se cortan y apuntan su elección en algún documento o se las auto-envían por correo para tenerlas a mano en caso de que la memoria falle. O de los que no siguen la recomendación de modificar su colección de credenciales de vez en cuando.

Una, dos y hasta tres credenciales

Para contener los efectos de este cóctel explosivo, las principales compañías de Internet están desplegando con ahínco toda una serie de servicios de verificación en dos pasos que suelen ser opcionales pero que, gracias a su activación, complican un poco la vida a los cibercacos. ¿En qué consiste la **verificación en dos pasos**, también llamada autenticación de dos factores? Como su nombre bien indica, esta solución **basa su fiabilidad en solicitar no una, sino dos**

claves diferentes a los usuarios antes de concederles pleno acceso a sus cuentas si se detecta una conexión no segura o un equipo diferente al habitual. Mientras una de ellas es la típica contraseña elegida por el dueño legítimo cuando se registra, la otra es un código que el sistema genera al azar en el momento de *loguearse*. Este código no se comunica en la misma página, sino que se envía a través de un mensaje de texto al teléfono indicado previamente por el usuario, cuando da de alta el servicio, o en ocasiones mediante una aplicación móvil.

De este modo, se le exige al internauta que proporcione **algo que sabe** o debería saber (su contraseña) y **una pieza alternativa que tiene** (el código que recibe en su dispositivo móvil y que acaba caducando con el tiempo), probando la veracidad de sus intenciones y minimizando los riesgos de suplantación de identidad. Y es que el *password* de toda la vida ya nunca más sería suficiente para ganar acceso a la información. Por si con dos acreditaciones no llegasen, también existen procedimientos que recurren a una tercera prueba para garantizar las conexiones: **algo que los usuarios son** y los diferencia del resto de la humanidad, como la huella digital, su voz o cualquier otro detalle biométrico que se pueda reconocer a través de un escáner.

Por supuesto esta técnica no es nueva, y no nos referimos a las proclamas de autoría de Kim Dotcom, que blande a su favor una patente concedida en el año 2000. La verificación en dos pasos es lo que se viene realizando desde hace tiempo con las tarjetas de crédito. Cuando alguien quiere retirar dinero desde un cajero necesita contar con el elemento físico de rigor (la propia tarjeta) y el que ha memorizado (el PIN). Asimismo, si se dispone a realizar una compra por Internet, al tecleo del PIN se le sumará la necesidad de añadir otro recurso como pueden ser el número de verificación de la tarjeta, su fecha de caducidad o incluso el código postal del dueño, o no se admitirá el cargo. Eso sí, que la autenticación de dos factores tenga largo recorrido en ciertas esferas como la financiera no significa que esté profusamente extendida por la Red.

De Google a LinkedIn

De hecho, esta capa de protección se está popularizando desde hace tan sólo unos meses en plataformas de correo electrónico y redes sociales, dos de los recursos cibernéticos más populares entre usuarios de todo el mundo. Uno de los primeros en implementarla, hace cosa de dos veranos, fue **Google** con el objetivo de fortalecer el acceso a los emails de **Gmail**, y a éste la siguió meses después **Dropbox**. Tras la polémica del borrado de la vida online de un periodista estadounidense a manos de los hackers, que eliminaron los datos contenidos en su iPhone, iPad y MacBook de forma remota , **Apple** ha aplicado la misma receta a **iCloud**. Y el tercer gigante por antonomasia, **Microsoft**, ha comprado PhoneFactor y ha asegurado las cuentas de **Windows**, **Windows Phone**, **Office**, **Outlook.com**, **SkyDrive**, **Skype** y **Xbox** con un *autenticador* que permite recibir códigos incluso sin conexión. Por su parte, **Azure** ha estrenado la Autenticación Activa que comprueba los inicios de sesión con una app móvil, una llamada telefónica o un SMS.

En la lista se encuentran asimismo **Evernote**, **Twitter** y **LinkedIn**, que se han puesto las pilas en materia de verificación en dos pasos tras sufrir embarazosos ataques hacker. El servicio de notas sólo ofrece el sistema, de momento, a usuarios de Evernote Premium y Evernote Business, aunque ha aprovechado para complementarlo con la disponibilidad universal de las Aplicaciones Autorizadas y el Historial de Accesos. La plataforma del pajarito azul ha bautizado su propuesta como "verificación de inicio de sesión", que depende del soporte de las distintas operadoras de telefonía. Y la red orientada a profesionales explica que "la mayoría de las cuentas de Internet que llegan a ser comprometidas son accedidas ilegítimamente desde un equipo nuevo o desconocido", y que eso se puede evitar con esta clase de iniciativas.

¿Qué dicen los más críticos?

La verificación en dos pasos se antoja una solución cómoda para los internautas y aparentemente segura para sus intereses, eso es cierto. Su existencia dificulta el acceso indeseado de terceros, pero no significa que las cuentas online que se sirven de ella estén completamente a salvo o se deban relajar las precauciones, y es justo por eso que tiene sus detractores. ¿En qué se basan las críticas en concreto? En primer lugar, en el hecho de que a pesar de la implementación de esta medida **continúa existiendo la fatalidad del robo físico de dispositivos y la posibilidad de arrancar el sistema en modo seguro** saltándose todas las barreras. O, aún más fácil, en que los datos quedan expuestos por la **mala costumbre de no cerrar sesión** justo al acabar de revisar el estado de una cuenta… desatando el debate de la dejadez de los usuarios una vez más.

Otro argumento que sigue esta línea es el que defiende que, por muchos controles que se realicen, las personas van a seguir cayendo en las **trampas de la ingeniería social, las técnicas "man-in-the-middle" y las elaboradas campañas de correo "phishing"**, que con el paso del tiempo se vuelven más sofisticadas para obtener la confesión voluntaria (pero bajo engaño) de las claves de acceso oficiales y las combinaciones de seguridad adicionales por parte de sus víctimas. También se advierte de las nefastas **consecuencias de no mantener actualizados con los últimos parches de software los ordenadores**, tabletas o teléfonos utilizados para conectarse a Internet, en los que se puede colar un troyano para escalar privilegios y hacer de las suyas, por no hablar del problema de la **recuperación de cuentas** o el hecho de **compartir credenciales para un mismo perfil corporativo** entre varios compañeros de trabajo, porque se desvanecen los límites de control.

Si todos estos escollos persisten, la verificación en dos pasos se entendería como una pieza más del puzzle de la seguridad, pero nunca como una solución definitiva que cortará de raíz los problemas "internetianos". Es más, existe la impresión de que, a medida que se vaya estandarizando a lo largo y ancho de los principales servicios de Internet, se perfeccionarán también aquellas técnicas de ataque que tienen los sistemas de autenticación como objetivo primordial, poniendo en entredicho su aparente invulnerabilidad. ¿Cuál es vuestra opinión al respecto? ¿Cuál creéis que es el futuro de la verificación en dos pasos? Os escuchamos.