Los límites entre seguridad y privacidad del usuario

Si hay algo de lo que me gusta debatir es precisamente de límites. De intentar ver el vaso medio lleno o medio vacío, entendiendo qué ganamos y qué perdemos en cada una de las decisiones que tomamos..., o toman terceros por nosotros.

Y en seguridad y privacidad de la información el encontrar ese Dorado que sería el equilibrio entre ambas patas da para escribir largo y tendido.

Esperar utilizar un sistema que sea 100% seguro, privado y usable, es utópico

Hay apaños, y la experiencia en el diseño de estos sistemas es un punto, pero por regla general, tendremos que decidir qué anteponemos.

Y el mejor ejemplo lo he vuelto a encontrar en un cambio que pasó sin más pena que gloria en la última versión de iOS, que entrara en circulación a finales del año pasado.

El control de seguridad debilita la privacidad de un sistema

Le meto mucha caña a Apple, precisamente, porque creo que de las grandes tecnológicas es la única que está remando en contra, anteponiendo más la privacidad del usuario, que la funcionalidad (y por tanto, negocio) de sus sistemas.

La estrategia de *pricing* de estos últimos años en Apple es fiel reflejo de esto. Los últimos iPhone son caros como producto unitario, ya que su precio viene dado por el valor que tiene acceder a su ecosistema[1]- más que un móvil, compras el acceso a una plataforma-, y sí, como siempre ocurriera con los productos de Cupertino, también el impuesto de ser un bien elitista, solo al acceso de un porcentaje de la sociedad[2].

Que al final estás pagando el gran esfuerzo que hace la compañía por ofrecer un entorno sensible a la privacidad y seguridad del usuario.

Algo que hacen, ojo, porque pueden. El negocio de Apple, al menos hasta el momento[3], es vender productos - hay que recordar que su pata de servicios superaba hace solo unos meses por primera vez a la venta de Macs, teniendo en cuenta que esto es algo puramente residual en un negocio que depende en exceso de la venta de iPhones-. El negocio de la competencia, sacar rédito a la explotación de datos de sus usuarios.

Unes ambos puntos y tienes la estrategia de posicionamiento esperable: "Nosotros protegemos tu privacidad". (Y ya de paso, añado la coletilla de "a diferencia de Google, Facebook, Microsoft y Amazon").

Y afortunadamente, no están vendiendo humo. El ecosistema de Apple es tan cerrado que facilita bastante el perseguir cualquier tergiversación por parte de terceros, y parchear cualquier vulnerabilidad en su ecosistema tan pronto es descubierta.

Lo que no quita que se les cuelen fraudes y haya malware enfocado en su plataforma. Pese a que tienen el mejor ecosistema (por lo cerrado que es) para controlarlo, no es ni técnica ni humanamente posible asegurar que algo no pasará los controles.

Pero vayamos al grano...

Sobre la puntuación de confianza en un sistema basado en el crowdsourcing

En la última versión de iOS entraba en juego un nuevo sistema que permite controlar posibles tergiversaciones de uso en iTunes.

Pablo F. Iglesias,
Consultor de Presencia Digital
y Reputación Online @PYDotCom

Estamos ante una nueva fórmula que tiene como objetivo mejorar la seguridad del sistema… a cambio de comprometer, aunque sea ligeramente, la privacidad del usuario.

Hasta aquí, todo normal. El problema es que para hacerlo, Apple utiliza resúmenes extraídos de las llamadas de teléfono e emails a los que asigna una puntuación de confianza[4]. De esta manera, asocia la identidad del usuario con el uso que da a funciones tan críticas como son las llamadas y los mails, lo que en principio podría utilizarse para identificar con mayor acierto a un usuario.

Por supuesto, todo este sistema entra dentro de esa privacidad diferencial[5] que es seña de identidad de los de Cupertino: "Apple no recibe información más allá de la puntuación, porque la información utilizada para determinar la puntuación se almacena en el dispositivo. Cada número de confianza generado por Apple está elaborado teniendo en cuenta los datos de miles de cuentas lo que hace que cada código sea único y se puede usar para determinar patrones de comportamiento raros en lo dispositivos".

Es decir, que ese valor se calcula dentro del dispositivo, y se comparte con los servidores de la compañía de forma cifrada y asociado únicamente a un identificador tokenizado. Lo que complica en exceso que un tercero, o incluso un trabajador de la compañía, pueda utilizarlo para identificar usuarios.

Lo complica, vaya. Que *impossible is nothing* ☺.

El caso, y es con esto con lo que quiero que te quedes, es que estamos ante una nueva fórmula que tiene como objetivo mejorar la seguridad del sistema... a cambio de comprometer, aunque sea ligeramente, la privacidad del usuario.

Que con este cambio seguramente damos un paso adelante[6] en esto de proteger al usuario de posibles fraudes. Pero también, a costa de añadir una capa extra que podría servir para identificar de una manera más atómica al usuario.

Que como decía hace tiempo, siempre hay grises en esto de explotar datos personales[7]. Los tiene Facebook[8], por supuesto. También Google[9], Microsoft[10] y Amazon[11]. Pero incluso una empresa como Apple, que se vanagloria de ser el adalid de la privacidad y protección del usuario, tiene que hacer concesiones[12].

Aunque no quede bonito, ni acapare titulares. ●

R.

1. https://www.pabloyglesias.com/jardines-vallados-ecosistema-movil/
2. https://www.pabloyglesias.com/apple-lujo-moda-y-tecnologia/
3. https://www.pabloyglesias.com/apple-pago-por-servicios/
4. https://nakedsecurity.sophos.com/2018/09/24/itunes-is-assigning-you-a-trust-score-based-on-emails-and-phone-calls/
5. https://www.pabloyglesias.com/inteligencia-y-privacidad/
6. https://www.pabloyglesias.com/sobre-proteccion-avanzada/
7. https://www.pabloyglesias.com/identidad-vs-privacidad/
8. https://www.pabloyglesias.com/espionaje-micro-smartphone/
9. https://www.pabloyglesias.com/la-excusa-privacidad/
10. https://www.pabloyglesias.com/privacidad-tecnologia-actual/
11. https://www.pabloyglesias.com/privacidad-y-asistentes-virtuales/
12. https://www.pabloyglesias.com/privacidad-diferencial-apple/