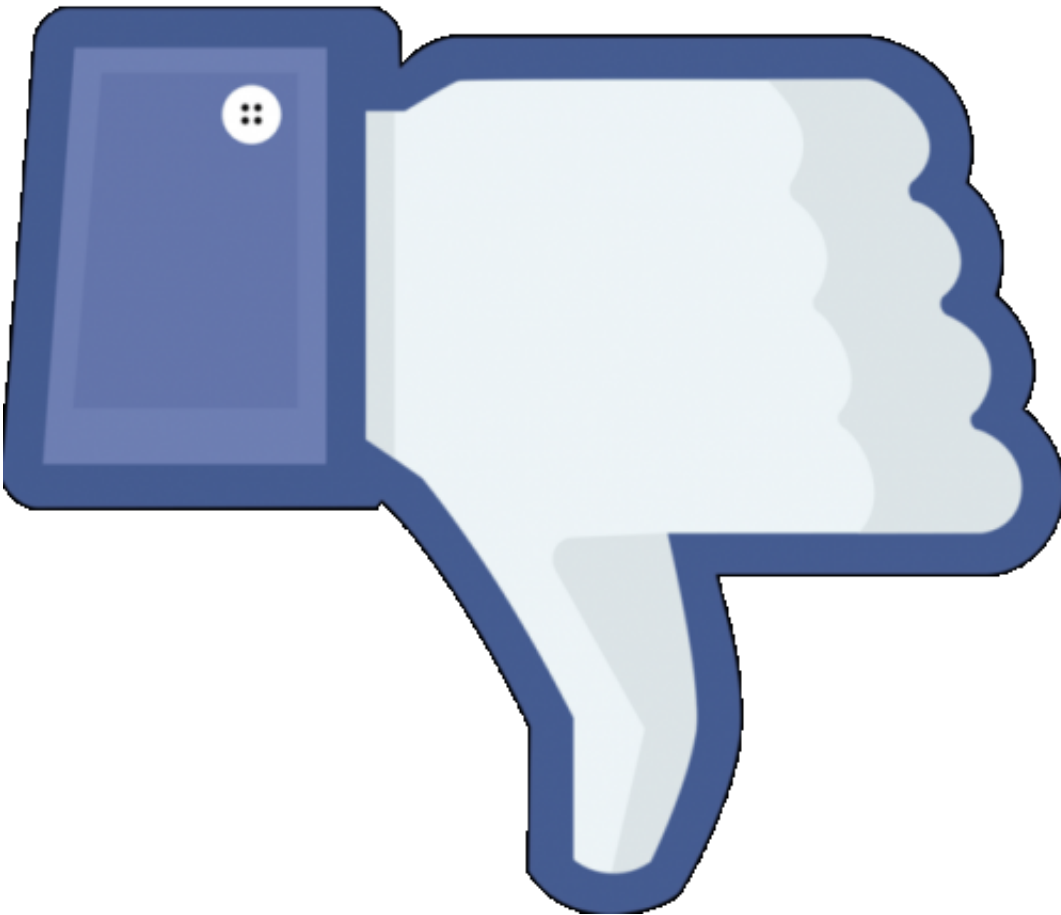


When Facebook goes down it takes big chunks of the internet with it

January 30 2015, by Ben Kirman And Tom Feltwell



It's not working for me. Credit: Kvarki1, CC BY-SA

Checking social networks is a morning ritual for many, and when that routine is disrupted – as it was recently when Facebook's servers went down – its absence [can come as a surprise](#). But what also becomes

apparent is that when the world's most popular social network is inaccessible, so too are many thousands of websites that rely upon Facebook services.

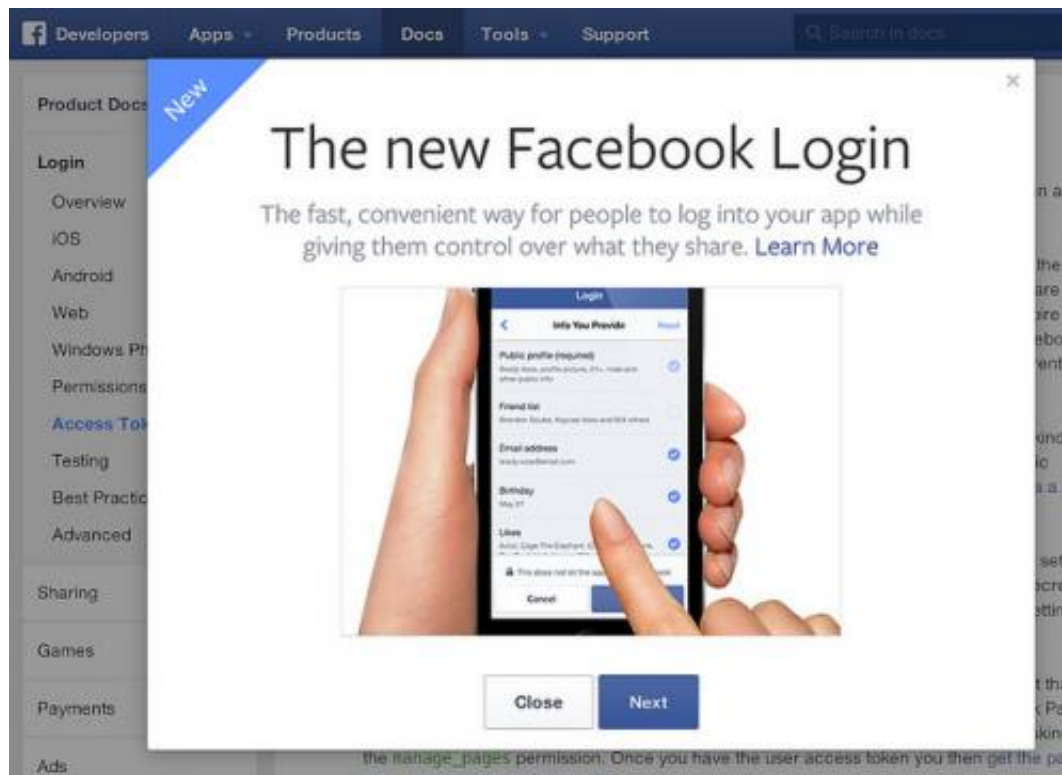
Although [it lasted less than an hour](#), Facebook's downtime gave a rare glimpse into the extent to which it – and other social networks – have penetrated our daily use of the web.

Instagram, [bought by Facebook in 2012](#), and Tinder, which requires a Facebook account to log in, were among the big sites that were also brought down. But many thousands of websites rely on a Facebook account as a means for users to log in or post comments – including The Conversation. This cascading failure shows how the need for websites to provide a means to authenticate users has given rise to a centralising trend – and the vulnerability to failure that brings.

Identity mistakes are costly

For the developer of a website or app user management is a difficult problem. You must be able to store, encrypt and decrypt users' information securely, allow them to reset their forgotten password, offer them a range of secret questions and other account management options. The more secure systems use two-factor authentication, which requires authentication via unconnected systems – for example combining username and password, mobile phone text message, fingerprint or keycard.

If not implemented perfectly correctly, user authentication can be vulnerable to abuse – as exemplified by the theft of intimate photos from celebrities' poorly secured Apple iCloud accounts last year, where attackers gained access by abusing password reset features and guessing simple passwords. If Apple can't get it right, what hope for your average developer?



Turning identity into a product - fine, until it stops working. Credit: factoryjoe, CC BY-NC-SA

Outsourcing identity

An appealing solution for developers is to outsource the problem to a third-party service. Back in the heady days of [Web 2.0](#) in the mid-2000s, this problem was first addressed with the development of [OpenID](#) – a distributed, open standard for authentication that could work across many sites and services. Users chose a single identity provider to securely hold their OpenID digital identity on their behalf, which third-party websites or services could use to authenticate them.

Initially popular, it fell out of favour with the rise of social networks as

companies realised the value in holding their users' identities themselves. Google will [stop supporting OpenID this April](#) in favour of the approach taken by Facebook, Twitter, LinkedIn and most other social networks. This will involve offering its own authentication service as part of a set of services and functionality aimed at developers, known as an application programming interface ([API](#)).

Using just a few lines of code, a developer can rely on a social network to carry out all the tricky user management business on their behalf leaving them to get on with building their app or website. As a bonus, using a social network API offers other features such as easy content sharing and demographic and social statistics. It seems like win-win-win exchange: the developer has less work to do, the user has a smooth log-in experience and the social media site parades its brand across a little more of the web, annexing a little more of online life.

When Facebook's down ... so are you

So the Facebook crash accidentally communicated a powerful but hidden message to millions of users: we own your online identity. Although news items may [jokingly mourn](#) for all the humblebrags and selfies lost that morning, we rely more and more on social networks to mediate our online existence. They are a vital source of both personal and global news, a source of social capital, define our personalities, manage our relationships and increasingly act as the social glue between our different haunts on the web. The companies controlling them have unprecedented access to much of our lives.

I'd imagine that the developers at Tinder – like many developers of other applications that rely on Facebook's authentication service – were summoned to emergency meetings this week as bosses realised exactly how dependent their business is on a third party out of their control.

We should take this brief disruption as opportunity to think about the extent that Facebook and its ilk own, control and facilitate our online lives – even far beyond their own sites. The disruption was short, but hints at the wider problems in the online identity business.

If you have thoughts, you can leave a comment. But as with most other news sites you have an important choice: will your identity on The Conversation belong to Twitter, Facebook or LinkedIn?

This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).

Source: The Conversation

Citation: When Facebook goes down it takes big chunks of the internet with it (2015, January 30) retrieved 9 April 2024 from <https://phys.org/news/2015-01-facebook-big-chunks-internet.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--