Should you pay for Meta's and Twitter's verified identity subscriptions? A social media researcher explains

March 8 2023, by Anjana Susarla

Credit: Pixabay/CC0 Public Domain

Social media services have generally been free of charge for users, but now, with ad revenues slowing down, social media companies are looking for new revenue streams beyond targeted ads. Now, Twitter is charging for its blue check verification, and Meta and Twitter both charge for identity protection.

Users benefit from "free" services such as social media platforms. According to one study, in the U.S., Facebook users say they would have to be paid in the range of $40 to $50 to leave the social networking service for one month. If you value Facebook highly enough that you'd need to get paid to take a break, why not pay for these new services if you can afford them?

Meta plans to offer paid customer support and account monitoring on Facebook and Instagram to guard against impersonators for US$11.99 a month on the web and $14.99 a month on iOS devices. Twitter's proposed changes make two-factor authentication via text messaging a premium feature for paid users. Twitter Blue costs $8 a month on Android devices and $11 a month on iOS devices.

As a researcher who studies social media and artificial intelligence, I see three problems with the rollout of these features.

The collective action problem

Information goods, such as those provided by social media platforms, are characterized by the problem of collective action, and information security is no exception. Collective action problems, which economists describe as network externalities, result when the actions of one participant in a market affect other participants' outcomes.

Some people might pay Facebook for improved security, but overall, collective well-being depends on having a very large group of users investing in better security for all. Picture a medieval city under siege from an invader where each family would be responsible for a stretch of the wall. Collectively, the community is only as strong as the weakest link. Will Twitter and Meta still deliver the promised and paid-for results if not enough users sign up for these services?

While large platforms such as Facebook and Twitter could benefit from lock in, meaning having users who are dependent on or at least heavily invested in them, it's not clear how many users will pay for these features. This is an area where the platforms' profit motive is in conflict with the overall goal of the platform, which is to have a large enough community that people will continue using the platform because all of their social or business connections are there.

Economics of information security

Charging for identity protection raises the question of how much each person values privacy or security online. Markets for privacy have posed a similar conundrum. For digital products in particular, consumers are not fully informed about how their data is collected, for what purposes and with what consequences.

Scammers can find many ways to breach security and exploit vulnerabilities in large platforms such as Facebook. But valuing security or privacy is complicated because social media users do not know exactly how much Meta or Twitter invests in keeping everyone safe. When users of digital platforms do not understand how platforms safeguard their information, the resulting lack of trust could limit the number of people willing to pay for features such as security and identity verification.

Social media users in particular face imperfect or asymmetric information about their data, so they do not know how to correctly value features such as security. In the standard economic logic, markets assign prices based on buyers' willingness to pay and sellers' lowest acceptable bids, or reservation prices. However, digital platforms such as Meta benefit from individuals' data by virtue of their size—they have such a large amount of personal data. There is no market for individual data rights, even though there have been a few policy proposals such as California governor Gavin Newsom's call for a data dividend.

Some cybersecurity experts have already pointed out the downsides to monetizing security features. In particular, in giving a very rushed timeline, one month from announcement to implementation, to pay for a more secure option, there is a real risk that many users will turn off two-factor authentication altogether. Further, security, user authentication and identity verification are issues that concern everyone, not just content creators or those who can afford to pay.

In the first three months of 2022 alone, nearly one-fifth of teens and adults in the U.S. reported their social media accounts getting hacked. The same survey found that 24% of consumers reported being overwhelmed by devices and subscriptions, indicating significant fatigue and cognitive overload in having to manage their virtual experiences.

It is also the case that social media platforms are not really free. The old adage is if you are not paying, then you are the product. Digital platforms such as Meta and Twitter monetize the enormous tracts of data they have about users through a complex online advertising-driven ecosystem. The system makes use of very granular individual user data and predictive analytics to help companies microtarget online ads and track and compare advertising views with outcomes. There are hidden costs associated with people's loss of privacy and control over their personal information, including loss of trust and vulnerability to identity theft.

Social media and online harms

The other problem is how these moves to monetize security options increase online harms for vulnerable users without identity protection provisions. Not everyone can afford to pay Meta or Twitter to keep their personal information safe. Social bots have become increasingly more sophisticated. Scams increased by almost 288% from 2021 to 2022, according to one report. Scammers and phishers have found it easy enough to gain access to people's personal information and impersonate others.

For those who are scammed, the process of account recovery is frustrating and time-consuming. Such moves might hurt the most vulnerable, such as those who need Meta to find access to job information, or the elderly and infirm who use social media to learn about what is happening in their communities. Communities that have invested resources in building a shared online space using platforms such as Twitter and Facebook may be harmed by monetization efforts.

People are tired of having to navigate numerous subscriptions and having security and privacy concerns that persist. At the same time, it's an open question whether enough users will pay for these services to boost collective security. Ultimately, the service a social media platform offers is the opportunity to connect with others. Will users pay for the ability to maintain social connections the way they pay for content, such as entertainment or news? Social media giants may have a difficult path ahead.

Provided by The Conversation

Citation: Should you pay for Meta's and Twitter's verified identity subscriptions? A social media researcher explains (2023, March 8) retrieved 25 April 2024 from https://techxplore.com/news/2023-03-pay-meta-twitter-identity-subscriptions.html