

[thedailybeast.com](https://www.thedailybeast.com)

'Beyond Sketchy': Facebook Demands Users' Email Passwords

Kevin Poulsen Sr. National Security Correspondent

4-5 minutes

Just two weeks after admitting it stored hundreds of millions of its users' own passwords insecurely, Facebook is demanding some users fork over the password for their outside email account as the price of admission to the social network.

Facebook users are being interrupted by an interstitial demanding they provide the password for the email account they gave to Facebook when signing up. "To continue using Facebook, you'll need to confirm your email," the message demands. "Since you signed up with [email address], you can do that automatically ..."

A form below the message asked for the users' "email password."

"That's beyond sketchy," security consultant Jake Williams told the Daily Beast. "They should not be taking your password or handling your password in the background. If that's what's required to sign up with Facebook, you're better off not being on Facebook."

In a statement emailed to The Daily Beast after this story published, Facebook reiterated its claim it doesn't store the email passwords. But the company also announced it will end the practice altogether.

"We understand the password verification option isn't the best way to go about this, so we are going to stop offering it," Facebook wrote.

It's not clear how widely the new measure was deployed, but in its statement Facebook said users retain the option of bypassing the password demand and activating their account through more conventional means, such as "a code sent to their phone or a link sent to their email." Those options are presented to users who click on the words "Need help?" in one corner of the page.

The additional login step [was noticed](#) over the weekend by a cybersecurity watcher on Twitter called "e-sushi." The Daily Beast tested the claim by establishing a new Facebook account under circumstances the company's system might flag as suspicious, using a disposable webmail address and connecting through a VPN in Romania. A reporter was taken to the same screen demanding the email password.

"By going down that road, you're practically fishing for passwords you are not supposed to know!," e-sushi wrote in a tweet.

Small print below the password field promises, "Facebook won't store your password." But the company has recently been criticized for repurposing information it originally acquired for "security" reasons.

Last year Facebook [was caught](#) allowing advertisers to target its users using phone numbers users provided for two-factor authentication; users handed over their numbers so Facebook could send a text message with a secret code when they log in. More recently the company drew the ire of privacy advocates when it began making those phone numbers searchable, so anyone can locate the matching user “in defiance of user expectations and security best practices,” [wrote](#) the Electronic Frontier Foundation, a civil liberties group.

Facebook also has a checkered history when it comes to securely handling passwords. Last month the company acknowledged that [unencrypted passwords](#) for hundreds of millions of its users [had been stored for years](#) in company logs accessible to 2,000 employees.

Last month, amid a steady drum beat of fresh privacy scandals, Facebook founder Mark Zuckerberg unleashed a thousand-word manifesto describing a new “privacy-focused vision” [for the company](#) built on strong encryption and cutting-edge security tools.

Even then, Zuckerberg acknowledged that Facebook’s putative pivot-to-privacy would meet with some skepticism. “[F]rankly we don’t currently have a strong reputation for building privacy protective services.”