

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

# Facebook is asking some new users for their email passwords and appears to be harvesting their contacts without consent

*Rob Price Apr 3, 2019, 3:10 AM*

5-6 minutes

- 
- **Facebook is asking some new users to provide the password to their email account.**
  - **The move has alarmed security experts, who warn it could encourage users to engage in "risky" behaviour and increase their chances of being hacked.**
  - **The social network also appears to be accessing these users' contacts without asking for permission.**
  - **The company now says it is discontinuing this login tool, though it didn't give a timeframe.**

Facebook asks some new users to provide the social network with the password to their email accounts, a move that security experts say has concerning security implications — and that could teach people to engage in "risky" behaviour online.

Typically, people are urged by security experts never to

share their passwords or enter them into any services other than the one for which they are intended, to avoid the risk of "phishing attacks" where users' passwords and personal information are stolen.

But on Facebook, when users try to register with certain email providers, including Yandex and GMX, it asks to "confirm your email address" by entering their password directly into Facebook, [as previously reported on by The Daily Beast](#). The issue was first discovered by pseudonymous Twitter user e-sushi.

—e-sushi (@originalesushi) [March 31, 2019](#)

Users of other email providers like Google's Gmail don't see the option, as it makes use of authorization tool OAuth — a common tool for securely verifying your identity without requiring you to input your password as Facebook is doing here.

Business Insider has also found that if a new user chooses to enter their e-mail account password into Facebook, a pop-up appears saying that Facebook is "importing contacts" — despite not asking the user for permission to do so. It is not immediately clear if this tool actually imports these contacts, as it apparently didn't pull in contact list entries we made for the purposes of testing, though these contacts were only minutes-old.

Screenshot/Rob Price

Reached for comment, a Facebook spokesperson said the company is now discontinuing the feature, though the company did not provide a timeframe.

### **'Basically indistinguishable from a phishing attack'**

Bennett Cyphers, a security researcher with advocacy group the Electronic Frontier Foundation, was harshly critical of Facebook's actions. "This is basically indistinguishable to a phishing attack," he said on a call, pointing out that people are ordinarily urged never to provide their passwords to anyone other than the site they were created from.

"This is bad on so many levels. It's an absurd overreach by Facebook and a sleazy attempt to trick people to upload

data about their contacts to Facebook as the price of signing up. Even when you consent to uploading contact information to Facebook, you should never have to put in your email password to do it," Cyphers wrote in a follow-up email.

"No company should ever be asking people for credentials like this, and you shouldn't trust anyone that does. This goes against all conventional security wisdom, basic decency, and common sense," he wrote.

Troy Hunt, a security expert and operator of the hack-notification-service Have I Been Pwned, was also critical. "It's certainly a security anti-pattern insofar as it involves sharing the secrets of one platform (the email provider) with another platform (Facebook)," he wrote in an email.

"Whilst Facebook would certainly be taking precautions to protect the email account password, it feels unnecessary when there's an easy alternative (i.e. the approach they take with Gmail accounts) and does condition people to partaking in risky behaviour," he wrote.

The password entry form says that passwords are not stored by Facebook, but there's no way to independently audit this and confirm that it's the case. [It was recently revealed that the company was storing hundreds of millions of users' passwords in plain text](#), in a violation of widely-held security best practices.

In a statement, a Facebook spokesperson said: "These passwords are not stored by Facebook. A very small group of people have the option of entering their email password to verify their account when they sign up for Facebook for the

first time. People can always choose instead to confirm their account with a code sent to their phone or a link sent to their email."

The spokesperson added: "That said, we understand the password verification option isn't the best way to go about this, so we are going to stop offering it."

---

**Got a tip?** Contact this reporter via encrypted messaging app Signal at +1 (650) 636-6268 using a non-work phone, email at [rprice@businessinsider.com](mailto:rprice@businessinsider.com), Telegram or WeChat at [robaeprice](#), or Twitter DM at [@robaeprice](#). (PR pitches by email only, please.) You can also [contact Business Insider securely via SecureDrop](#).