Want a new Facebook account? Just hand over your private email password

4-5 minutes

Just when you thought Facebook couldn't get more invasive, the social network has been caught asking new users for the password to their email accounts. Sure, what could go wrong? It's not like that info will end up in the cloud…

After clicking the email verification link, some fresh Facebook users were asked for their private email password – a cybersecurity no-no that should cause even the most naïve internet user to recoil in horror. It's unclear when this innovation in intrusiveness was introduced, or how long it lasted as a feature, but its existence was confirmed by the Daily Beast after it was exposed by Twitter sleuth @originalesushi.

Hey @facebook, demanding the secret password of the personal email accounts of your users for verification, or any other kind of use, is a HORRIBLE idea from an #infosec point of view. By going down that road, you're practically fishing for passwords you are not supposed to know! pic.twitter.com/XL2JFk122l

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

Facebook sheepishly admitted they were indeed demanding passwords, but protested users could "*bypass*" the password-request screen by clicking the "*need help?*" link and triggering a multistep process that would eventually allow them to confirm using "*more conventional*" means, such as a DNA sample – er, a phone code. They also said they were very, very sorry and would stop asking for email passwords in the future.

While Facebook promised it doesn't store users' email passwords, a privacy promise from Facebook isn't worth the pixels it's printed with, as even CEO Mark Zuckerberg [admitted](#) last month when he piously announced the company would finally focus on protecting users' data, "*because frankly we don't currently have a strong reputation for building privacy protective services.*"

[Also on rt.com Facebook stored 7 years of passwords in plaintext, but it's OK, they're trustworthy!](#)

After all, it was Facebook that stored half a billion users' passwords on its servers in unencrypted plaintext for seven years - then told users not to worry, because its employees were trustworthy (those employees who weren't calling the users "*dumb f**ks,*" that is). And it was Facebook that [collected](#) users' phone numbers for "*security purposes only*" – then violated their trust by making profiles searchable by phone number and offering the data to advertisers so they could more effectively target users. But Zuckerberg [declared](#) privacy dead in 2010! Why are we still moping over its

corpse?

Lest Facebook get all the blame for spreading users' data where it isn't supposed to be, cybersecurity firm UpGuard found over half a billion Facebook "*records*" – account names, comments, and reactions – exposed and downloadable on open-access Amazon cloud servers owned by Mexican news-and-culture site Cultura Colectiva, while an app called At the Pool had left 22,000 email addresses, names, and, yes, passwords on open cloud servers after the company went under.

[Also on rt.com 'We're sorry this happened': Bug causes leak of 7 million Facebook users' photos](#)

While it's likely this user data was slurped up pre-Cambridge Analytica – when Facebook's rules for how apps could use their data primarily consisted of "*don't get caught*" – third-party app developers had access to this kind of data for years before the regulatory attention spurred by that company's legendary transmutation of user data into votes inspired Facebook to begin auditing thousands of apps to ensure they weren't "*mishandling*" user information in their own way.

A Facebook spokesperson [told](#) Bloomberg that the company's policies "*prohibit storing Facebook information in a public database.*" And we can trust them. Right?

Helen Buyniski

Think your friends would be interested? Share this story!