securityboulevard.com

Facebook Forces Users to Give Email Password (wait, what?) - Security Boulevard

by Richi Jennings on April 3, 2019

7-9 minutes

Here's Facebook's latest unbelievable scandal: The company has been demanding that some users enter their email passwords, so they can be "verified."

That's right, their *email* password. Facebook claims it's all above board: It's for security, y'see—people can totally trust us. But critics say it trains users to do dangerous things.

And Facebook is said to be harvesting the users' contacts without permission. All this just a month after the company was caught red-handed misusing other security identifiers. Yikes.

Facebook also claims that users can instead verify their email an alternate way, but the UX for that seems to be a blackest-of-Vantablack "dark pattern." In today's SB Blogwatch, we can't believe our eyes.

Your humble blogwatcher curated these bloggy bits for your entertainment. Not to mention: 挑戦 (DERA).

Facebook Facepalm FAIL

What's the craic? We need to talk about Kevin Poulsen —"Facebook Demanding Some New Users' Email Passwords":

> Mark Zuckerberg admitted recently that Facebook doesn't have a 'strong reputation' for privacy. An odd new request for private data probably won't help with that rep.
> …
> Facebook is demanding some users fork over the password for their outside email account as the price of admission. … In a statement … Facebook reiterated its claim it doesn't store the email passwords.
> …
> 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. … More recently the company drew the ire of privacy advocates when it began making those phone numbers searchable.
> …
> 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.

It gets worse: That is, if Rob Price is right. He claims Facebook "appears to be harvesting their contacts without consent":

> [It's] a move that security experts say has concerning security implications — and that could teach people to engage in "risky" behaviour online. … When users try to register with certain email providers, including Yandex and GMX, it asks to [enter] their password directly into Facebook.
>
> …
>
> 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.
>
> …
>
> The company now says it is discontinuing this login tool, though it didn't give a timeframe. … "We understand the password verification option isn't the best way to go about this, so we are going to stop offering it."

And worse still: Tom McKay wins the headline war—"Just Casually Asking Some New Users for Their Email Passwords," while pointing out the dark pattern:

> It is never, **ever** advisable for a user to give out their email password to anyone, except possibly to a 100 percent verified account administrator when no other option exists (which there should be). Email accounts tend to be primary gateways into the rest of the web, because a valid one is usually necessary to register accounts on everything from banks and financial institutions to social media.
>
> …
>
> They obviously also contain copies of every un-deleted message ever sent to or from that address, as well as

> additional information like contact lists. It is for this reason that email password requests are one of the most obvious hallmarks of a phishing scam.
> …
> A Facebook spokesperson confirmed in a statement … "People can always choose instead to confirm their account with a code sent to their phone or a link sent to their email." … However, those other options could only be reached by clicking the "Need help?" button … which is not an obvious manner of communicating that there are other options.
> …
> Facebook has also in the past issued contradictory statements about what kind of data it collects (such as call data and app usage) … launched pseudo-VPN apps that vacuumed up user data, and seemingly obfuscated how users could control whether it obtains call and text data.

Who discovered this utter stupidity? e-sushi —@originalesushi—tastes raw emotion: [You're fired—Ed.]

> 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!
> …
> Also, there is no alternative to verify. This is practically a "give #Facebook the secret password to your personal email account, or bust" kinda thing.
> …
> This is the "please verify you're a benign human" screen

> that pops up right after registering. … Stumbled upon it yesterday. Replicated it today.
> …
> Tested it myself registering 3 times with 3 different emails using 3 different IPs and 2 different browsers. 2 out of 3 times I faced that email password verification thing right after clicking “register account” on their front page sign up form.
> …
> So far, my testing shows gmx.net, gmx.de, and mail.com tend to trigger it. … Today I got word from a friend he faced the same thing last week.

This is fine? kyle-rb wonders who is sitting calmly, surrounded by flames:

> I just don’t understand how this gets implemented without someone speaking up and saying “hey, wait, isn’t this an insane thing to do?”.
> …
> Some combination of the complainers being ignored, and people at a higher level thinking “well we’re doing this in a secure way, as long as the user trusts us, and why wouldn’t they trust us, we’re Facebook!”

And unionpivo expands on the “risky lesson” angle:

> It has been established as minimal practice, that **no one** should be asking you about your password. If this would become a normal, it would also make regular people more likely to give out their passwords.
> …

> Email is key to your online kingdom, so it's a big deal.

But newnewpdro thinks that ship has sailed:

> The general public is extremely **myopic** and **lazy**. They will hand over anything you ask for if it means they have to do less work.
> …
> Convenience trumps all. It's how we've ended up with people voluntarily purchasing, maintaining, carrying around at all times, keeping charged and powered on, their own personal surveillance devices running heaps of software they have no control over.

So, try not to get close to SmellyGeekBoy:

> I … haven't logged on to Facebook since new year's eve, I was a very heavy user before that. 4 months in and I haven't missed out on anything.

Meanwhile, Noah Shachtman snarks it up:

And Finally:

挑戦 (DARE) but beats 2 and 4 are swapped

You have been reading SB Blogwatch by Richi Jennings. Richi curates the best bloggy bits, finest forums, and weirdest websites… so you don't have to. Hatemail may be directed to @RiCHi or sbbw@richi.uk. Ask your doctor before reading. Your mileage may vary. E&OE.

Image source: Alessio Jacona (cc:by-sa)

— Richi Jennings

Recent Articles By Author