securityweek.com

Facebook Demanded User Email Passwords

Tags: NEWS & INDUSTRY Privacy Identity & Access

6-7 minutes

Facebook has been found asking users for their email passwords. A screen form told users that their email address needed to be confirmed in order to update their contact information, and suggested that it could be done via gmx.net. All the user needed do was enter their email account password into the Facebook form.

When independent security consultant and researcher Mike Edward Moras (e-sushi on Twitter) discovered this, he immediately tweeted, "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!"

In fact, when he first saw the form, he thought he had landed on a phishing page. "It looked like one of those phishing pages one can find when following email spam links," he told *SecurityWeek*. "But this was Facebook itself, on its main domain, being served via SSL with a valid

certificate. This wasn't some weird malware thing; they genuinely were asking me for my password to a 3rd party service -- the password that logs me in to my email provider."

Last month, Facebook CEO Mark Zuckerberg published an open memo claiming that Facebook would become more privacy conscious in the future. He said, for example, "People expect their private communications to be secure and to only be seen by the people they've sent them to -- not hackers, criminals, over-reaching governments, or even the people operating the services they're using." And yet this request could expose the entirety of users' email communications to one of 'the people operating the services they're using'.

With little understatement, Zuckerberg commented in the same memo, "I understand that many people don't think Facebook can or would even want to build this kind of privacy-focused platform -- because frankly we don't currently have a strong reputation for building privacy protective services..."

The media rapidly picked up on Moras' tweet, and made his concerns public knowledge. In fairness, Facebook reacted swiftly, and responded, ìWe understand the password verification option isnít the best way to go about this, so we are going to stop offering it,î it said. But this doesn't explain why or how it happened.

"The fact that companies like Facebook have their own security as well as infosec teams, raises the question why

this went live without internal protest," comments Moras. "Therefore, it has to be assumed this was not an 'accident' or anything they hadn't thought through before pushing to public." A more common approach to email account verification is to email that account with some form of response request. This confirms the validity of the account without requiring the user's credentials.

Moras told SecurityWeek that the page was live for at least 96 hours before being removed, and he believes that during that period, some users will have provided their passwords. He hopes that Facebook will have deleted these, because the security dangers are severe.

"With full access to an email account, almost anything is possible," Moras told SecurityWeek. "Every credential that passes through your inbox suddenly has to be considered as 'leaked to Facebook'. It could even go so far that your email account could be used to sign you up for something you don't even know exists -- and Facebook could not only sign you up for it, they could also verify your email, and remove all traces of this so you wouldn't know until it is too late do anything about it.

"In the other direction," he added, "any service or website you signed up for using that email has to be considered 'potentially breached' as credentials could be passively harvested by Facebook, in a worst case allowing them to access the private/protected data you store at those services and websites without your consent and, again, without you noticing it before it is too late to prevent

damage."

Only Facebook knows how long the page was active before being 'discovered'. "We can only trust in Facebook they won't abuse such data and that they actually deleted those passwords as stated [at the bottom of the form]," he said. "Then again, Facebook doesn't have a reassuring track record when it comes to being trustworthy in privacy realms."

Zuckerberg has already admitted this, and recent history beyond this password snafu confirms it. Facebook is already facing several GDPR investigations in Europe. It was found culpable in the Cambridge Analytica scandal and fined £500,000 by the UK data protection regulator; and is under investigation by the FTC for possible breach of a 2011 consent order.

In February 2019 it was reported that certain phone apps send sensitive user data -- including health information -- to Facebook. In March 2019 it emerged that the company had stored hundreds of millions of Facebook and Instagram users' passwords in plaintext. And in April 2019, more than 540 million records containing data on Facebook users and their activities were discovered in an unprotected AWS S3 bucket.

Related: Facebook Faces Criminal Probe of Data Deals: Report

Related: 'Digital Gangsters': UK Wants Tougher Rules for Facebook

Related: Is Facebook Out of Control? Investigations and Complaints Are Rising

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: