Historic Breach from Facebook Groups
This is a statement under embargo until Monday February 18

- A group of patients and cybersecurity experts have filed an FTC complaint against Facebook, claiming that the largest breach of health data ever occurred from Facebook's Groups product.
- The FTC complaint claims that Facebook is liable for tens of billions of dollars in fines for the breach due to failing to notify Facebook users of the breach under the FTC PHR Breach Notification Rules.
- The vulnerability that the patient group discovered applies to many of Facebook's closed groups that support potentially targeted populations, including Veterans, Police Officers, Churches and Religious Communities.
- Online support groups play a widespread role in the healthcare system, providing essential peer support to people dealing with myriad health challenges.
- For health-related peer support groups on everything from living with diabetes, to parenting a child with autism, to dealing with a cancer diagnosis, by far the most utilized online platform is Facebook, with millions of people participating in clinically-focused Facebook groups.
- Millions of people in closed groups on Facebook share a great deal of personal and sensitive information, including clinical information, in order to obtain the support and information they need.
- In early 2018, the patient community began investigating the privacy and security settings in Facebook after the Cambridge Analytica scandal.
- In April 2018, Andrea Downing, a moderator of a closed support group for cancer previvors and survivors, discovered security flaws that could allow private information in the group to leak to non-members. A security researcher, Fred Trotter, confirmed that this dangerous vulnerability exposed patient data for millions of patient users in closed groups. Andrea and Fred named the security vulnerability "SicGRL."
- In May 2018, Downing and Trotter detailed this serious vulnerability in a 40 page report they submitted to Facebook through its "white hat portal", with support from other healthcare data cybersecurity experts.
- In late June, Facebook modified its Closed Group privacy settings, addressing one dangerous permutation of SicGRL. Facebook publicly denied that they made this change to address any privacy problem in response to the vulnerability report. More importantly, Facebook also denied that there was any leak of patient data at all.
- Facebook has yet to fully fix the security problem with their groups platform, and the breach of healthcare data from the platform is ongoing.
- Fred Trotter and other cybersecurity experts estimate that the ongoing data breach as the result of SicGRL is the largest breach of healthcare data in the history of the Internet, impacting millions of patients and other vulnerable people worldwide.
- MissingConsent.org is a new website that explains the risks for patient users in communicating on healthcare topics on Facebook.

Previous Headlines On this Story For Reference:

- CNBC
- Wired
- Atlantic
- BoingBoing

New Developments 02.03.19:

- Due to Facebook's continued refusal to address the remaining SicGRL vulnerabilities, the security researchers and patient advocates who discovered the problem submitted a complaint to the FTC in December.
- Given that the FTC has recently been closed due to the government shutdown, and might soon be again, we have decided to go public with
    - The redacted version of the FTC complaint.
    - The redacted SicGRL vulnerability report that we provided to Facebook
    - The Facebook reply to SicGRL vulnerability report, which states "we do not consider it to be a privacy or security concern in the product."

Please consider this FTC complaint to be embargoed until 1:00 am Monday February 18th.

Fred Trotter Statements:
(Fred's Bio)

"Facebook has decided that FTC regulations that apply to other systems that host patient data for patients do not apply to them, despite actively encouraging patients to use their products in a way that is clearly covered by FTC regulations."

"Facebook has weaponized Artificial Intelligence to profit from patient groups. Facebooks UX continually pesters patients to join Facebook groups based on hints that patients accidentally give to Facebook. If you visit the American Cancer Society's Facebook page, Facebook will guess that you are a cancer patient, and encourage you to join cancer-related Facebook groups. By joining, patients confirm to Facebook that they do have a particular clinical condition, which allows Facebook to sell targeted ads against that new information. The fact that the healthcare status of those Facebook users is made public is something that Facebook seems to regard as an irrelevant side-effect."

"Talking with Facebook privacy team is frustrating. Their position is in fact "hey, these groups are not safe for patients to use" but that is not what they actually say. Instead, Facebook's employees have learned a kind of "privacy doublespeak"; the wording ends up sounding like, "our products are not ideal for every use-case", but what they mean is that they have no intention of improving privacy controls to make patients safe. And this frustrating conversation continues as Mark Zuckerberg continually promotes the product for use by patients in keynotes.

"There has never been a breach of healthcare data this large. This is the first time that an Internet platform has published healthcare information, using real names, of people across the planet. The number of people impacted are in the millions, and it is impossible to avoid the conclusion that some of the people who are impacted have been subjected to physical violence, snake-oil treatments and targeted harassment that likely resulted in casualties in at least some cases."

"This is not a different problem from the violence in Myanmar or from Russian hackers attempting to arrange violence in Houston. All of these are driven by the underlying flaw in Facebook groups security that is documented in the SicGRL vulnerability"

Andrea Downing Statement:

(Andrea's Bio)

"Moderators of many of patient support groups have spent years working to ensure these are safe spaces for their members. Everyone, including me, trusted that the Facebook's group platform is a safe safe for support. I have learned that patients need to *trust but verify*"

"We have done everything we possibly can to help Facebook's leadership understand the severity of this security problem with SiCGRL and Closed Groups. The company is well aware of the fact that vulnerable groups are in harm's way. Rather than do the right thing, Facebook swept this under the rug."

"Other journalists have provided evidence of how information gathered on social media can be used to deny people jobs and healthcare. No one has yet connected this back to the massive amounts of data being shared in closed groups. The very groups patients created as a lifeline to help and support each other through traumatic experiences can be used against members.'

"Without acknowledging the dangers of SicGRL vulnerability, Facebook's head of Healthcare Research published in a major medical journal in December about the benefits of mining health data on Facebook to make clinical decisions."

"After reporting these problems through the proper channels at Facebook, you can imagine my shock to see a Facebook employee co-authoring papers about the benefits of mining this health data in a reputable medical journal."

"To date, I have not seen any meaningful discussion or public dialogue about the scale and severity of problems with Facebook's group platform. The public needs to understand how Closed Groups can be weaponized."

"At first I didn't believe Fred when he said that the problem with groups can cause a loss of life. I thought to myself, *but this is just social media.* Now I understand things differently, after I have been studying Facebook groups for 8 months. I am afraid for the safety of our community, and wish we could move somewhere else."

"For patient support groups on Facebook, the bottom line is that we can be easily hacked, scraped, and deleted at anytime. We brought this problem to Facebook and they have swept it under the rug. Facebook knows how dangerous this is for vulnerable groups, and we've made every attempt to give them information and evidence to fix the problem."

"People easily forget that Facebook was the "privacy aware" alternative to MySpace over a decade ago. Now, we are working on ways to leave the platform and collectively self-govern the data generated by Closed Groups. Hopefully other patient groups will join us by finding ways to prevent this from happening again."