ALL DATING SITES NOW HACKED OR SELLING YOUR DATA TO GOOGLE! ALL YOUR SEXUAL SECRETS ARE NOW EXPOSED ON-LINE!

By David Goldman and Jose Pagliery @CNNTech

Hear a revenge porn hacker explain why he did it

Hear a revenge porn hacker explain why he did it

More than 3.5 million people's sexual preferences, fetishes and secrets have been exposed after dating site Adult FriendFinder was hacked.

Already, some of the adult website's customers are being identified by name. Adult FriendFinder asks customers to detail their interests and, based on those criteria, matches people for sexual encounters. The site, which boasts 64 million members, claims to have "helped millions of people find traditional partners, swinger groups, threesomes, and a variety of other alternative partners." The information Adult FriendFinder collects is extremely personal in nature. When signing up for an account, customers must enter their gender, which gender they're interested in hooking up with and what kind of sexual situations they desire. Suggestions AdultFriendfinder provides for the "tell others about yourself" field include, "I like my partners to tell me what to do in the bedroom," "I tend to be kinky" and "I'm willing to try some light bondage or blindfolds." The hack, which took place in March, was first uncovered by independent IT security consultant. Bev Robb on her blog Teksecurity a month ago. But Robb did not name the site that was hacked. It wasn't until this week, when England's Channel 4 News reported on the hack, that Adult FriendFinder was named as the victim. ***Are you concerned that your private information has been exposed? Tell us your story.***

Included in the exposed personal information are customers' email addresses, usernames, passwords, birthdays and zip codes, in addition to their sexual preferences. No credit card data has yet been uncovered as part of the hack. That data is incredibly revealing and potentially damaging. Andrew Auernheimer, a controversial computer hacker who looked through the files, used Twitter to publicly identify Adult FriendFinder customers, including a Washington police academy commander, an FAA employee, a California state tax worker and a naval intelligence officer who supposedly tried to cheat on his wife. Millions of others remain unnamed for now, but anyone can open the files -- which remain freely available online. That could allow anyone to extort Adult FriendFinder customers.

For instance, the security consultant Robb reported that one person whose information was hacked was a 62-year-old Hispanic male from New Jersey, who worked in advertising and has a preference for the "subporno" forum. That, combined with his username and other account details, gave Robb enough information to Google him, find his real name, and find his social media pages. The information exposed can be particularly devastating to people living in small towns, where they are more easily identified.

For example, one person exposed in the hack is a 40-year old welder from a small Illinois town of a few thousand people. He "will become anybody's slave" and lied about his age on the site, claiming to be 29. The breach was carried out by a hacker who goes by the moniker ROR[RG]. In an online hacker forum, he said he blackmailed Adult FriendFinder, telling the site he would expose the data online unless the company paid him $100,000. On the forum, hackers immediately praised ROR[RG], saying they

were planning on using the data to attack the victims. "i am loading these up in the mailer now / i will send you some dough from what it makes / thank you!!" wrote a hacker who goes by "MAPS." FriendFinder Networks Inc., parent company of Adult FriendFinder and other adult sites and publications including Penthouse, said in a statement that it had just become aware of the breach, and it is working closely with law enforcement and cyberforensics company Mandiant, a FireEye (FEYE) subsidiary.

The company said it doesn't yet know the full scope of the breach, but it promised to "work vigilantly," noting that FriendFinder Networks "fully appreciates the seriousness of the issue." "We cannot speculate further about this issue, but rest assured, we pledge to take the appropriate steps needed to protect our customers if they are affected," the company said. Related: Selling your Android phone? Don't. Related: Massive Clinton-era Internet bug shows pitfalls of Obama's 'backdoor' proposal

CNNMoney (New York)

FAKE DATING PROFILES: EXPOSED!

CLICK BELOW, TO LEARN MORE FROM THE SITE DEDICATED TO ENDING THIS PRACTICE: bigfakes