THE WALL STREET JOURNAL.

http://www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152

TECH

Hackers Target Users of Infidelity Website Ashley Madison

Cyberattack could expose millions of users' personal information

By **DANNY YADRON**
Updated July 20, 2015 7:43 p.m. ET

The lesson from the latest cyberhack of personal data: Arranging marital infidelity online carries all the risks of its real-world counterpart.

The parent company of Ashley Madison, a dating site aimed at those looking for extramarital affairs, confirmed on Monday that its systems were hacked by an intruder threatening to release the real names and personal preferences of the site's millions of users unless it shuts down.

The hackers said they obtained account holders' names, addresses and other personal information.

On its website, Ashley Madison claims more than 37 million "anonymous members," though it is unclear how many of those are active, individual users.

Although the intruders, who refer to themselves as "Impact Team," released the identities of some purported Ashley Madison users Sunday night, no new data was released Monday and the site remained operational.

"We apologize for this unprovoked and criminal intrusion into our customers' information," Toronto-based Avid Life Media Inc. said in a statement. "At this time, we have been able to secure our sites and close the unauthorized access points."

Avid Life said it forced file-sharing sites to take down samples of the stolen data. However, the company declined to discuss what data the hackers still have. Avid Life, which runs several other niche dating sites, has said in recent months it is considering

going public.

A spokesman said that remains an option “irrespective of today’s news.”

Ashley Madison’s home page made no mention of the breach, but instead touted a “trusted security award” and that Ashley Madison is a “100% discreet service.”

The problem, at least for some people, is that operators of the consumer Internet still haven’t figured out how to keep sensitive information truly secure. This year, hackers also broke into a database of sensitive user data for AdultFriendFinder.com.

It remains unclear how the hackers got in or what security measures the site had in place. The company said it hired Cycura, a cybersecurity company, to investigate the breach. Cycura declined to comment Monday.

The Royal Canadian Mounted Police declined to comment.

The breach came to light Sunday night after the hackers—or possibly hacker—messaged computer security blogger Brian Krebs.

The message included a manifesto against Ashley Madison, and samples of files the hackers said had come from Ashley Madison’s network.

In their letter, still available online Monday, the hackers accused Ashley Madison of misleading users on the types of data it collects.

For $19, the company offers a service called “Full Delete” for departing customers that will remove things like a profile from the site, any messages a user has sent or received, photos and usage history. The hackers allege that since users pay for this service with a credit card, the site maintains records that those users were customers.

“We have all such records and are releasing them as Ashley Madison remains online,” the hackers wrote.

In a written statement, Avid Life disputed this.

“Contrary to current media reports, and based on accusations posted online by a cyber criminal, the ‘paid-delete’ option offered by AshleyMadison.com does in fact remove all information related to a member’s profile and communications activity,” the company said.

The company also said that, “we are now offering our full-delete option free to any member, in light of today’s news.”

Avid Life declined to comment on the veracity of specific pieces of user data that the hackers claim to have, other than referring to it as “personally identifiable information.”

“I have to take them at their word,” Mr. Krebs said in an interview Monday, citing “the extent of the access they had.”

Well-known for his coverage of other data breaches, such as those at Target Corp. and Home Depot Inc., Mr. Krebs said Avid Life executives appeared to be aware of the breach before he contacted them Sunday night.

Mr. Krebs quoted Avid Life Chief Executive Noel Biderman as saying the hack was done by “a person here that was not an employee but certainly had touched our technical services.”

Avid Life declined to make Mr. Biderman available for an interview Monday.

In many high profile breaches, the hackers steal the username and password of someone with access to corporate systems.

This allows them to steal data without quickly tripping alarms.

—Maureen Farrell contributed to this article.

Write to Danny Yadron at danny.yadron@wsj.com

Corrections & Amplifications:
AdultFriendFinder.com is owned by FriendFinder Networks. An earlier version of this article incorrectly stated that it was owned by Avid Life Media. (July 20, 2015)