Snapchat: Will make app more secure

January 3 2014, by Barbara Ortutay

This Thursday, Oct. 24, 2013 file photo shows Snapchat CEO Evan Spiegel in Los Angeles. Snapchat, the disappearing-message service, has been quiet following a security breach that allowed hackers to collect the usernames and phone numbers of millions of its users. Snapchat said Thursday, Jan. 2, 2014 that it is assessing the situation, but did not have further comment. Earlier in the week, hackers reportedly published 4.6 million Snapchat usernames and phone numbers on a website called snapchatdb.info, which has since been suspended. (AP Photo/Jae C. Hong)

(AP)—Snapchat says it plans to put out a more secure version of its application following a breach that allowed hackers to collect the

usernames and phone numbers of some 4.6 million of its users.

The disappearing-message service popular with young people said in a blog post late Thursday that the updated version of its app would allow users to opt out of its "Find Friends" feature, which was apparently at the heart of the breach, and would stem future attempts to abuse its service.

The breach occurred after security experts warned the company at least twice about a vulnerability in its system.

Before announcing its plans to update the app, Snapchat had been quiet. Its seemingly detached response caused some security specialists to wonder whether the young company can handle the spotlight that it's been thrust into over the last year as its service has become enormously popular.

In response to a warning by Gibson Security on Dec. 25 —which followed an earlier alert in August—Snapchat said in a blog post last Friday that it had implemented "various safeguards" over the past year that would make it more difficult to steal large sets of phone numbers. Snapchat hasn't detailed the changes it made.

As Americans rang in the New Year, hackers reportedly published 4.6 million Snapchat usernames and phone numbers on a website called snapchatdb.info, which has since been suspended. The breach came less than a week after the most recent warning from security experts that an attack could take place.

The incident bruises the company's image and may threaten its rapid growth. Los Angeles-based Snapchat has no source of revenue, but its rapid rise to an estimated 20 million U.S. adult users prompted Facebook to extend a reported $3 billion buyout last year. Snapchat's 23-year-old CEO Evan Spiegel turned down the overture. The user number estimate

is based on census data and data from the Pew Research Center.

What should users do? Gibson Security, the firm that warned Snapchat of the security vulnerability on Christmas Day, has created a site,—lookup.gibsonsec.org/—that lets users type in their username to see if their phone number was among those leaked. Of two user accounts that The Associated Press checked, one was found to have been compromised.

Gibson Security did not publish the last two digits of the phone numbers.

Gibson says users can delete their Snapchat account if they wish, but "this won't remove your phone number from the already circulating leaked database." Users can also ask their phone company to give them a new phone number.

"Lastly, ensure that your security settings are up to scratch on your social media profiles. Be careful about what data you give away to sites when you sign up—if you don't think a service requires your phone number, don't give it to them," Gibson said.

This was Gibson's second warning to Snapchat, following one in August that the security firm said was ignored.

"Given that it's been around four months since our last Snapchat release, we figured we'd do a refresher on the latest version, and see which of the released exploits had been fixed (full disclosure: none of them)," Gibson wrote on the Gibson Security website.

The Snapchat breach comes just two weeks after Target was hit with a massive data security breach that affected as many as 40 million debit and credit card holders.

Gartner security analyst Avivah Litan said phone numbers are not considered "sensitive" personally identifiable information—such as credit card or social security numbers—so they are collected by all sorts of companies to verify a person's identity.

A phone number is "not as bad as password or magnetic strip information, but it's the piece of the puzzle that criminals need to impersonate identities," she said.

Christopher Soghoian, principal technologist with the American Civil Liberties Union, agreed.

"The main problem was that they ignored a responsible report by security researchers," he said, adding that his concern is not with the specific database of information that was released, but that Snapchat has "demonstrated a cavalier attitude about privacy and security."

Many people use Snapchat because it feels more private than other messaging apps and social networks. Users can send each other photos and videos that disappear within a few seconds after they are viewed. While the recipient can take a screenshot of the message, a big draw of Snapchat is its ephemeral nature.

"This probably won't be the last problem with Snapchat," Soghoian said. Companies like Microsoft and Google, he added, actively court security researchers and even pay bounties for people to expose flaws in their systems.

"Snapchat may be too small to pay bounties, but they certainly should be treating researchers with respect and addressing issues as soon as they are told about them," he said.

In its blog post Thursday, Snapchat listed an email address that security

experts could use to contact the company "when they discover new ways to abuse our service so that we can respond quickly to address those concerns."