**Home Depot Says Hackers Also Stole Email Addresses**

**By**

**[NICOLE PERLROTH](http://bits.blogs.nytimes.com/author/nicole-perlroth/%22%20%5Co%20%22More%20Posts%20by%20Nicole%20Perlroth)**

 NOVEMBER 6, 2014 6:38 PM November 6, 2014 6:38 pm 18

Photo



Home Depot said hackers used the user name and password of one of its vendors to gain a foothold in its computer systems.Credit Toby Talbot/Associated Press

The hackers that broke into Home Depot’s computer network this year took 53 million customer email addresses in addition to the payment card details for millions of customers, the company announced on Thursday.

When the company [first confirmed in September](http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/) that its computer systems had been breached, it said someone had gained access to credit card information and other personal data for 56 million of its customers — the largest known breach of a retailer.

The email addresses could be used in phishing attacks, in which hackers send malicious links or attachments or try to trick people into giving them more valuable information, like passwords.

The company also settled another mystery. Until now, it was not publicly known how hackers had managed to get into its systems. But on Thursday, Home Depot said someone used the user name and password of one of its vendors to gain a foothold, then broke into different parts of Home Depot’s systems, including a database of customer emails and the company’s in-store cash register systems.

The company did not say which of its vendors the hackers used to gain access. According to a government report from July, [hackers have been looking](http://www.nytimes.com/2014/07/31/technology/checking-in-from-home-leaves-entry-for-hackers.html) for new ways to gain entry into the computer networks of American retailers. One way is through vendors that have access to the network the hackers want to penetrate.

In the [breach at Target](http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html) last year, for example, hackers managed to break in through the retailer’s heating and cooling management company. In other cases, hackers have broken in through a range of third-party systems, from those to manage human resources to[employees’ favorite Chinese restaurants](http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html).



Customers checking out at a Home Depot in California in 2010. This year, hackers stole 53 million email addresses in an attack.Credit David McNew/Getty Images

Until the [Target](http://topics.nytimes.com/top/news/business/companies/target_corporation/index.html?inline=nyt-org) breach was exposed in December, former Home Depot employees say, Home Depot did not take an aggressive approach to data security, relying on outdated software and [ignoring warnings from employees](http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html). But the company said the malware that was used to steal data from its systems had never been used before the breach and would have been difficult for its antivirus systems to detect.

Home Depot said it had since plugged holes in its systems and would alert customers whose email addresses were compromised. After the Target breach, the company also began adding tough encryption of payment data in its United States stores, in which hackers would acquire only indecipherable gibberish in place of card information.

Home Depot said encryption was completed in its United States stores on Sept. 13 and would be finished in its Canadian stores early next year.

Home Depot also said it would adopt chip-and-PIN technology, which uses a microchip and a personal code to make it more difficult for hackers to use the payment details collected from one merchant for any future attacks or to counterfeit credit cards.

The payment card industry has set a soft deadline of October 2015 for United States merchants to switch to chip-and-PIN technology. Home Depot has said its project will be completed before then.