

Cyber Aware CASE STUDY



...they failed to update their security software...three years prior to the breach.

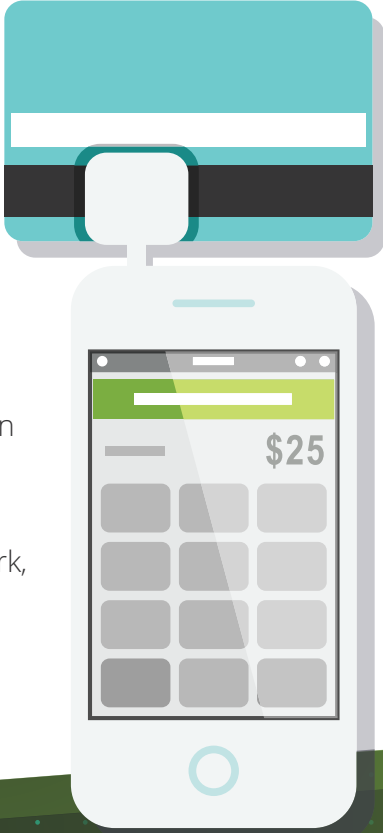
HOME DEPOT

Hours after compromised credit card information appeared for sale online, the U.S. Secret Service contacted Home Depot.




Upon further investigation, Home Depot announced that 56 million

customer credit and debit card accounts were stolen, along with 53 million customer email addresses.

The Home Depot attack had similar markings to a breach of Target's network, including entry into the network via a third party username and password.



Had they implemented two-factor authentication (2FA), which requires another piece of information such as a card, fob, or biometric, they would have added another layer of protection. Home Depot also failed to update its security software; it was still using Symantec's 2007 Endpoint Protection 11, which should have been upgraded three years prior to the breach.

-  **APRIL 2014**
Using credentials (username and password) from a third party vendor, hackers gained access to the perimeter of Home Depot's network.
Once in the network, the hackers exploited a zero-day vulnerability. This previously unknown weakness within Microsoft Windows enabled them to escalate privileges, move laterally through the network, and identify 7,500 self-checkout lanes.
-  **JUNE 2014**
The hackers deployed custom-built malware on the self-checkout system that stole customer credit and debit card information and email addresses.
Data was exfiltrated during business hours so as not to alert Home Depot's security team.
-  **SEPTEMBER 2014**
Credit and debit card information was offered for sale on an online underground cyber crime shop. The email addresses were presumed to be used in phishing schemes, attempts to trick recipients into revealing sensitive information.
Later, the Secret Service notified Home Depot that they traced credit card numbers for sale back to Home Depot.

