Consumers urged to be vigilant in wake of Zappos cyberattack

January 18 2012

(PhysOrg.com) -- As an estimated 24 million Zappos.com customers begin receiving notifications that some of their personal data have been compromised in a massive cyberattack, an Indiana University cybersecurity expert is warning those affected to be on the lookout for targeted fraud attempts.

Sunday's announcement by Zappos that customer accounts had been compromised by an unknown attacker poses serious risks for consumers, according to Maurer School of Law Distinguished Professor Fred H. Cate.

Efforts by Zappos CEO Tony Hsieh to reassure affected customers of his online shopping site that "customers' critical credit card and other payment data was not affected," run the risk of misfocusing the public attention and understating the risk, Cate said.

"Credit cards are covered by a federal law that limits consumer liability in the case of fraud up to $50, and card issuers universally waive even that small amount," he said. "Compromised credit card data is not the major area for concern."

Instead, according to Cate, who also serves as director of the IU Center for Applied Cybersecurity Research, the data that were reportedly accessed in the Zappos breach -- customer names, addresses, phone numbers, email addresses and encrypted passwords, in addition to the last four digits of customer credit card numbers -- pose the greatest risk

to affected individuals. That risk falls into three categories.

First, this information is precisely that used by fraud perpetrators to send fraudulent phishing emails purporting to come from legitimate businesses to individuals. "Think about it," Cate said. "If you get an email from a company that includes your correct name and contact information and refers to the last four digits of your credit card number, wouldn't you think it is real?

"In fact," Cate continued, "it is not at all clear how customers will be able to distinguish real messages from fraudulent emails claiming to come from Zappos itself."

Second, this is exactly the information necessary to locate other data about individuals in public and commercial records.

"If I have your name, address and phone number, in many states I can get your property tax records, marriage license and other publicly available information," Cate said. "With that additional information a criminal is in an even better position to commit frauds in your name or to access password-protected sites by using the extra information to answer password-reset questions."

Third, since the information included emails and encrypted passwords, this poses a serious risk to other online accounts held by affected customers of Zappos.

"Almost all consumers reuse passwords, and email addresses often serve as default account names for online sites, so depending upon the quality of encryption being used by Zappos, it is entirely possible that the perpetrators will have access to a wide range of online accounts," Cate said.

Fortunately, most major breaches do not result in extensive fraud. In addition, there are practical steps consumers can take to protect themselves, including:

-- Changing passwords on all accounts that used the same passwords compromised on the Zappos site.
-- Using unique passwords on all online sites.
-- Monitoring account, credit card and bank statements carefully.
-- Paying special attention to emails received, especially those claiming to be from businesses for which the consumer may have used the same credentials.

Provided by Indiana University