Zapping Identity Breach Problems

1/30/12

By: Administrator

The recent announcement by online shoe-seller Zappos that a hacker may have gained access to some of its customers' data is a reminder that our personal information can be vulnerable even if we shred our documents, put our bill payments in public mailboxes, use firewalls and anti-virus and anti-spyware on our home computers, and take the other recommended steps to protect it. When we provide our data to others, it's up to them to keep it safe.

Zappos immediately notified its customers, even though, from what we know at this point, the data in question wouldn't have triggered state data protection law notice requirements (it appears that no Social Security numbers or driver's license numbers were involved, and only the last four digits of customers' credit card numbers were exposed). Any breach causes valid concerns, however, so the notice was a good move. With other information that the hacker may have obtained, such customers' names, email addresses, billing and shipping addresses, and phone numbers, identity thieves might try to get into their accounts. They could also launch "phishing" attacks, pretending to be from Zappos, law enforcement agencies, credit card issuers, or other trusted parties to try to trick the customers into revealing more sensitive information.

The email notice that Zappos sent to customers was well designed: it was short and to the point, it used humor to relieve anxiety about the situation, and it described exactly what type of data may have been compromised. It also instructed customers to take action by changing their passwords. In fact, Zappos forced them to do so by disabling their old passwords, even though the passwords that the hacker may have accessed were cryptographically scrambled to make them very difficult for anyone else to read them. Another good move on the company's part was not to include a link to its website in the email. In phishing scams, emails designed to look just like those of legitimate companies usually contain links that take consumers to imposter websites, where they're instructed to provide their personal information. It's a common online safety tip not to click on links in emails that arrive unexpectedly, since they may be phishing attempts or contain stealth programs designed to capture people's passwords and other sensitive information. In this case, Zappos did the right thing by simply telling customers to go to Zappos.com to change their passwords.

The notice could have been improved by warning customers about phishing scams and describing how they work. Zappos did not tell customers to put fraud alerts on their credit reports, and that probably makes sense because it's unlikely that the compromised data could result in new credit accounts being opened in the names, which is what fraud alerts

are meant to deter. But it might have been helpful to suggest that if customers use their Zappos passwords on other accounts, they should change them as well. And it's important for Zappos customers, and all consumers, to monitor their existing accounts carefully and be vigilant for any signs of possible identity theft. Privacy Rights Clearinghouse provides good advice for consumers about How to Deal with a Security Breach. For businesses and other entities that store consumers' data, the California Office of Privacy Protection's Recommended Practices on Notice of Security Breach Involving Personal Information is an excellent resource.