

## Phishing Alert - Watch For Fraudulent Package Delivery Emails

---

The recent Target data breach made everyone sit up and take notice. Initially, news reports said about 40 million credit and debit cards may have been affected when hackers broke into the point-of-sale (PoS) systems and stole credit card information and PINs from the swipe pads in Target stores. The investigation later determined that the stolen information — acquired through malware in the PoS systems — included names, mailing addresses, phone numbers, or email addresses for up to 100 million individuals. What's more, Target is not alone. Adobe and LivingSocial are among other businesses that also experienced major data breaches in 2013.



What's the takeaway from the Target data breach? Security experts suggest the following:

- **On a daily basis**, go online to check your credit card statements for unfamiliar purchases as well as your bank account for fraudulent transactions. Report any problems immediately to your bank. (Your bank should contact you if your credit card was part of the Target breach. You'll get a new credit card account number and won't be held liable for unauthorized charges made using your credit card number.)
- **Check for suspicious activity** by reviewing your free credit report at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com). You should also report suspected fraud to law enforcement or to the Federal Trade Commission (FTC) at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).
- **Plan for the worst and take preventative steps.** Create strong passwords that would be hard for hackers to guess should they steal your account numbers. Also, do not use the same password for every account.

Target says its guests will have zero liability for the cost of any fraudulent charges arising from the breach and is offering one year of free credit monitoring and identity theft protection to all guests who shopped its U.S. stores. More details are available at [www.target.com/databreach](http://www.target.com/databreach).