

Fake Airline Ticket “Phishing” Scam

A new e-mail “phishing” scam seeks to plant malicious software on the computers of recipients who open an attachment purportedly related to the purchase of an airline ticket.

The fake e-mails use the names of various U.S. airlines including Northwest Airlines, Continental Airlines, Sun Country Airlines, US Airways, Allegiant Air, Delta Air Lines, Alaska Airlines, Midwest Airlines, and Hawaiian Airlines.

The e-mail messages urge recipients to confirm a ticket purchase they never ordered. The email requires an entry by thanking recipients for buying the tickets using the “Buy flight ticket online” service offered by the airline. Giving fake details of the purchased ticket, it asks them to confirm the purchase by printing the invoice and the ticket after clicking on an attachment in the mail.

However, when unsuspecting recipients click on the e-mail, a malicious software program downloads onto their computers. This “malware” enables the fraudsters to gain confidential information such as credit card access codes, Social Security numbers, and net banking passwords by allowing them remote access to the computers.

Airlines say there are a couple of things inside the mail that should warn people of the scam.

The e-mails contain mistakes in spelling and grammar, and the formats in which the itineraries are presented are different than those used by the airlines.

Members should be aware that these e-mails are not coming from the airline. If the format does not look familiar to you, and you have not recently purchased a ticket, do not open the attachment. Delete the e-mail right away.

Below is an example of an e-mail received by a credit union executive:

From: Hawaiian Airlines [\[mailto:tegoo@qq.com\]](mailto:tegoo@qq.com)

Sent: Thursday, November 13, 2008 4:24 PM

To: James Mxxxx

Subject: Your flight ticket

Dear Valued Customer

Thank you for using our new service ‘Buy airplane ticket Online’ on our website.

Your account has been created:

Your login: 1mooreDacu.com

Your password: PASS8QBE

Your credit card has been charged for \$424.85.

We would like to remind you that whenever you order tickets on our website you get a discount of 10%!

- Report suspicious Internet sites and emails to the government and for additional protection tips visit www.ic3.gov or the Federal government's consumer information center at www.consumer.gov/Tech.htm.
- A good resource for this topic is Anti -Phishing Working Group at <http://www.antiphishing.org/index.html>.
- If you have been victimized by a spoofed e-mail or web site, you should contact your local law enforcement, US Postal Inspector, or FBI.