

home about us careers search contact us sign out

CUNA MUTUAL GROUP
INSURANCE • SERVICES • ASSET MANAGEMENT

welcome **my services** products international my profile

Resource Center Home

RISK Alerts

Report a RISK Alert
Loss Prevention Lib.
Plastic Card Library
Policy Change Info

New 'Phishing' Scam Uses Fake Airline Ticket

November 21, 2008

Summary

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.

State(s): All States

Type of Alert: Phishing

[Loss Prevention Recommendations](#)



Get notified of high risk deposits and payments, as well as suspicious identities.

CUNA Mutual alerts credit unions of this risk. Please pass this information on to all appropriate employees. If your credit union has experienced a loss, contact our Credit Union Protection Response Center at 1.800.637.2676.

Details:

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 e-mail 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.

You and your 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]
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%!

*Attached to this message is the purchase Invoice and the airplane ticket.
To use your ticket, simply print it on a color printed, and you are set to take off for the journey!
Kind regards,
Hawaiian Airlines*

Loss Prevention Recommendations:

- Educate your membership on "Phishing, Smishing, and Vishing."
 - Post warnings on your Web site, in newsletters, and in branch lobbies.
 - Post a notice on your credit union's Web site, stating that you will NEVER solicit personal or private information via e-mail.
 - Educate your members if they have doubts about who's on the phone, call back the number of record at your financial institution or Card Company.
 - Advise your members to be wary of any message received from an unknown sender.
 - Educate your members to not open unsolicited e-mails or text messages.
 - Advise your members to not click on any links provided in unsolicited e-mails.
 - Encourage your members to monitor financial accounts on a regular basis.
 - Educate your members to deploy "blockers" on emails, text messaging, phone numbers, both land line and VoIP. In addition, consider "extra" caution when using "text messaging". Your member may want to disable the "text messaging" feature on their mobile device if they are not using it. Don't display your wireless phone number or e-mail address in public. This includes newsgroups, chat rooms, Web sites, or membership directories.
 - Educate your members to check the privacy policy when submitting their wireless phone number or e-mail address to any Web site. Find out if the policy allows the company to display or sell your information.
- If a member is a victim of Phishing, Smishing or Vishing, take appropriate steps:
 - Block and reissue the compromised credit/debit cards or the account that is at risk.
 - If not blocking the at risk card number or account, utilize an authorization strategy to prevent fraud exposure.
 - Have your member report the incident to the credit bureau.
 - Encourage your member to order a credit report.
- 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.

If you are aware of a risk in your area, whether it has struck your credit union or not, please complete the [Report a RISK Alert](#) form.

The information contained in this RISK Alert is intended for the sole use of our Credit Union Bond policyholders to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

CUNA Mutual Group does not provide any warranties or guarantees with respect to the performance of services by any vendor, and is not liable for any products or services purchased from any vendor by any credit union. Each credit union is ultimately responsible for determining the products and services that it may require, selecting the vendor that best meets the credit union's needs (whether or not a preferred partner), and contracting directly with that vendor.