Airline Travelers Beware - New Scam Targeting Frequent Flyers

December 5, 2011 - Whether you book your airline tickets for business or pleasure, if you purchase your airline tickets online, there is a new scam targeting you. It is a phishing attack that appears to be setup to steal your personal information and gain access to credit card numbers. It could also lead to you being locked out of your frequent flyer information and having your mileage completely drained.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The attack is fairly simple and is designed to easily manipulate potential victims into opening an attached file. Victims are notified of a ticket purchase. Obviously, if you haven't purchased an airline ticket and you get a message stating that one has been purchased in your name, you may feel compelled to investigate by clicking on the attachment or links within the mail message. By the same token, if you fly frequently and you receive a message like this, you may actually assume that the message is legitimate, and then click on links in the letter or open the attachment. Either way, you could be in trouble.

Multiple versions of this scam are now being circulated by e-mail. Last month, there was a report that a Delta Airlines version of the attack was circulating that made it very difficult for victims to determine that they had been duped. Apparently this version of the scam has a number of legitimate Delta Airlines links along with links to various US government websites. Once a consumer is convinced that the e-mail is legitimate, they are much more likely to open the attachment.

Another version that we're aware of appears to come from American Airlines. This one is much less elaborate but may be quite effective. Victims here simply receive a plain text message that comes from an aa.com e-mail address. (aa.com is used by American Airlines.) The message contains a flight number, an electronic ID number, a date and time for the

flight, the flights destination and a cost for the flight. Interestingly enough, it doesn't contain a departure city or any reference to the name of the passenger.

The message goes on to say, "Please find your ticket attached."

American Airlines is aware of the messages and does have a section of their website that addresses them. The airline is very clear that it does not send tickets in attached files. They go on to say that anyone receiving a message like this is clearly being told by American that the message should be deleted and that under no circumstances should links be clicked on or attachments be opened.

Anyone who does fall victim to this scam is likely to find themselves locked out of their frequent flyer account. In that event, victims should contact the airline by phone and have their account password reset. They should also check to make sure that their account balance is accurate. If they have credit cards associated with their account, they also need to make sure that no purchases have been made in their name; either through the airline or one of the airline's affiliates.

ACCESS is unaware of any airline sending out tickets in an attached file. Confirmation of ticket purchase is normally contained in the body of an e-mail message from airlines. Any message from any airline that contains an attached file supposedly for printing your tickets should be considered dangerous. If you are concerned that someone may have gained access to your account information and purchased a ticket in your name, then pick up the phone and call the airline and speak with a live agent about the issue. Don't click on links or attachments within the message regardless of how tempted you may be.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter: