Follow Us on Twitter

May 23, 2013

Fraud Alert – Memorial Day Holiday Weekend

The upcoming holiday weekend will find fraudsters using phishing emails to obtain agents' GDS login IDs and passwords to issue tickets – typically high-dollar cash tickets for immediate departures. Be on the lookout for any emails claiming to be from your GDS or a well known tour operator. Below you'll find a recent phishing email example followed by important instructions.

From: Travelport [mailto:support@wspan-emea.com]
Sent: Friday, May 17, 2013 11:57 AM
To:
Subject: Login Portal Update

Worldspan Go! Res Login Portal Update

5/17/2013,

The Worldspan Go! application have changed ,It's now featuring Travelport Smartpoint App technology . Because of these important changes , All users are required to confirm their Login informations . Please Confirm your unique sign-in and Password .

Please click here to confirm your Sign-in

Never confirm your GDS credentials through an email, and use extreme caution when clicking any links!

Effective Date : 06/01/2013 - all global countries
Note: **Unconfirmed sines will be locked**

Travelport Support.

Some noticeable errors in spelling, spacing, punctuation, and capitalization are highlighted in yellow.

Follow Us on Twitter

What should you do with this information?

1. Show this example of a phishing email to everyone, including full- and part-time staff, independent contractors and sub-agents.
2. Ask every employee, or outside sales staff if they received this type of email and if they clicked the link and logged into the GDS through the email. If so, take immediate action to change everyone's passwords, and refer to your GDS's website for additional instructions.
3. **Advise staff to never click on a link and confirm/enter a GDS login ID or password through an email** – always go directly to your GDS's known website.
4. If the agency's GDS administrator's credentials were compromised, check to see if new user accounts have been created or if any user's email account information has been altered. (Always delete unknown or former user accounts immediately.)

Monitor your agency's ticketing daily, including weekends and **holidays**, and if you suspect unauthorized ticketing or access, **immediately**:

- Void the ticket(s) through your GDS to obtain an ESAC code.
- Notify affected carriers of the unauthorized/stolen tickets.
- Cancel the PNR (or return segments if the outbound leg has been used).
- Contact your GDS to report compromised IDs, PCCs, or passwords, and ask for immediate assistance to prevent additional unauthorized activity.
- Contact ARC's fraud prevention team at fifp@arccorp.com or **(855) 358-0393** for important follow-up instructions.

More on current schemes, fraud prevention and credit card transaction red flags can be found at:
https://www.arccorp.com/support/fraud-prevention.jsp

ARC will send more examples of suspect emails in the future to keep you informed of the latest fraud attempts. Don't forget to follow us on Twitter.

About ARC:

As the financial backbone of the travel industry, ARC enables commerce among travel agencies, airlines, and travel suppliers, and offers them secure and accurate financial settlement services. ARC also supplies transactional data to organizations, facilitating better business decisions through fact-based market analyses. Established in 1984, ARC is headquartered in Arlington, Virginia. For more information, visit www.arccorp.com.

Contact:
Need to report fraud? Have questions about fraud?
+1 703.816.8137
+1 855.358.0393
+1 703.816.8138
fifp@arccorp.com
3000 Wilson Boulevard, Suite 300
Arlington, VA 22201-3862

# # #

©2013 Airlines Reporting Corporation (ARC). All rights reserved.