



## EMAILS POSING AS YOUR GDS – PHISHING FOR PINS AND PASSWORDS

Agents are reporting the receipt of phishing emails that appear to be from their GDS – but they are NOT, they are from a fraudster trying to entice you to provide sensitive information about your organization - both personal and/or business. The fraudster's aim is to gain access to your GDS by getting you to provide details of your login IDs, pseudo city codes, passwords, PINS and other sensitive information.

Upon receipt of this information, the fraudster(s), without your knowledge, may access your GDS and begin ticketing whilst you are not looking, using your office identification as a means to gain access to inventory and electronic tickets.

The fraudsters are clever in that they are using the logos of the GDSs and so it looks genuine. Here is an example: note the wording, spacing and misspellings (logos are removed from this example which was used without authorization).

- Original Message -

From: Travelport

To:

Sent: Wednesday, February 15, 2012 4:14 PM

Subject: Global Sign-in Update

**Worldspan Go! Res and Galileo GDIA Sign-in Update**

2/15/2012 ,

Travelport is adding a new level of security at time of signing into the reservations system. All users are required

to enter a unique Sign-in and a Password when they sign into Worldspan and Galileo GDIA . Sign-in passwords are

mandatory for all locations.

**Please click here to confirm your Sign-in**

Effective Date : 2/30/2012 - all global countries

Note: **Unconfirmed sines will be locked**

Travelport Support.

This email was sent to

We respect your right to privacy. This email was sent by Travelport GDS

© 2011 Travelport. All rights reserved. All Travelport trademarks and other proprietary materials used herein are the property of Travelport and/or its affiliates.

Please note that GDSs will NEVER ask you to reveal any login IDs or passwords, or ask you to confirm your usage via emails of this nature.



So what should you do to protect yourself?

- **DO NOT CLICK** on any of the links.
- **ASK** every employee, independent contractor, sub-agent or outside sales staff if they have received any type of phishing email and used the link presented to 'login to your account immediately'. If so take immediate action to change that person's user password and notify your GDS for any additional instructions.
- **AUDIT** all of your active user accounts and disable or delete user accounts that are no longer active (e.g. former employees). If you find an unknown user account immediately change your administrator's password. Use a complex password including capital letters, numbers and symbols combinations. Contact your GDS for additional suggestions.
- **WARN** your staff NEVER to click on a URL contained in an email – tell them to go to the original site.
- **REVIEW** your bookings and ticketing in your GDS early each day (including weekends and holidays) for spikes in sales, high-risk itineraries, unfamiliar booking patterns for cities that you do not usually book and high ticket values, particularly First and Business class sales. If you suspect unauthorized ticketing or access to your agency location has taken place act IMMEDIATELY:
  - Void the tickets through the GDS to obtain an ESAC code if you can,
  - Notify all the affected carriers, particularly the Validating Carrier,
  - Cancel the remaining reservations in the PNR,
  - Contact your GDS immediately to report compromised IDs, PCCs, Passwords and/or unauthorized ticketing/access and ask for immediate assistance to stop and/or prevent additional unauthorized ticketing or access,
  - Advise your local BSP Customer Services team via the IATA Customer Services Portal Contact for any follow up action.

**Please circulate this alert to everyone to prevent fraud.**