Follow Us on Twitter

March 7, 2013

Example of New Phishing Email

Here's an example of a recent phishing email sent to agents to obtain their GDS login IDs and passwords to issue tickets – typically high-dollar cash tickets for immediate departures. Be on the lookout for any emails purporting to be from your GDS and follow the **important instructions following this newest example of a current phishing email.**

From: Sabre Inc [mailto:donoreply@sabre.com]
Sent: Tuesday, March 05, 2013 1:36 PM
To:
Subject: Sabre System Notice Online Maintenance
Importance: High

MySabre

- **System Notice Online Maintenance**

Sabre Portal is currently down for *maintenance* .To provide a better quality of services to these clients, Sabre is updating a new level of security into the Sabre Red Workspace
Once you are logged in, Sabre will be automatically updated.
Please connect to Mysabre to confirm your system:

Effective Date : 03/31/2013 - all global countries

Note: **Unconfirmed agent ID will be locked**

Sabre Travel Network

.

What should you do with these examples?

1. Show these examples to everyone, including full- and part-time staff, independent contractors and sub-agents.
2. **Advise everyone not to enter their GDS login ID or password through an email** – always go directly to your GDS's known website.

Follow Us on Twitter

3. Ask every employee, or outside sales staff if they received this type of email. If so, take immediate action to change everyone's passwords and refer to your GDS's website for additional instructions.
4. If the agency's GDS administrator's credentials were compromised, check to see if new user accounts have been created or if emails for any user have been changed. (Always delete unknown or former user accounts immediately.) Contact your GDS to see if additional steps should be taken.
5. Review your bookings and ticketing in your GDS early each day for unauthorized ticketing.

If you suspect unauthorized ticketing or access, **immediately**:

- Void the ticket(s) through your GDS to obtain an ESAC code.
- Notify affected carriers.
- 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 ticketing or access.
- Contact ARC's fraud prevention team at fifp@arccorp.com or 855.358.0393 (toll-free) 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 U.S. travel industry, ARC enables commerce among travel agencies, airlines, and travel suppliers, and offers them secure and accurate financial settlement services. About 16,000 travel agencies and 190 airlines make up the ARC network. In 2011, ARC settled more than $82 billion worth of transactions between travel sellers and airlines. ARC also supplies transactional data to organizations, facilitating better business decisions through fact-based market analyses. Established in 1984, ARC is headquartered in Arlington, Va. For more information, visit www.arccorp.com.

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

# # #