Follow Us on Twitter

March 14, 2013

New Twist: Corporate Accounts Receive Phishing Emails

Several agents have again confirmed the use of compromised credit cards for tickets that appear to be for their corporate account. (See ARC's previous fraud alerts dated Dec. 23, 2010 and April 19, 2012 on ARC's fraud prevention pages). Employees of corporate accounts are receiving phishing emails that appear to be from their company, instructing them to click on a link within the email to log in, giving access to the company's website and online booking tools. Tickets worth thousands of dollars have already been issued on compromised credit cards for same/next day travel, usually in and out of African airports or other international departures.

You may want to consider advising your clients of this new twist in fraudsters gaining access to your client's website and/or their on-line booking tools. Although phishing emails may all be a little different, they typically:

- Appear to be from the company
- Display the company logo
- Advise the reader that email and calendar services have been updated
- Provide multiple links for the reader to:
  - Receive new information on how to access their email
  - Obtain urgent information
  - Confirm their login ID and password for a new level of security

Agencies should review their corporate account transactions and not assume that all tickets are genuine simply because they originate from a known customer. You may also want to consider after-hours response capabilities for callers needing access to the online booking tool, password resets, etc.

Assign someone to **review all GDS ticketing daily, including weekends and holidays**, analyzing both the current and previous day's bookings and tickets looking for:

- Spikes in sales (cash and credit)
- Immediate (same or next day) departures
- Changes in a corporate client's usual travel patterns (e.g. same/next day departures, international departures, etc.)
- Use of the "guest" booking feature for known corporate clients
- Use of unknown credit cards
- Unusual origins and destinations
- High-dollar tickets
- High risk itineraries (e.g. international departures to/from West African airports like ABJ, ACC LOS, CMN)

What to do if you identify some of these changes in patterns or suspect compromised credit cards:

- Take immediate action to verify legitimate passenger names and credit cards with your corporate account.
- **Act quickly to properly void the tickets** through your GDS to obtain the ESAC code from the carrier's e-ticket database.

Follow Us on Twitter 

- Cancel (**do not refund**) return segments of the ticket that may have been used outbound to reduce losses.
- Determine how access to your corporate account's online tool may have occurred and initiate appropriate follow-up actions to prevent further such access.
- Review online booking tool rules and settings with each corporate account to identify or lessen any vulnerabilities.
- Contact ARC's Fraud Prevention department for important follow-up information at fifp@arccorp.com or (855) 358-0393.

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

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?
+1 855.358.0393
+1 703.816.8138
fifp@arccorp.com
3000 Wilson Boulevard, Suite 300
Arlington, VA 22201-3862

# # #