Warning: Fraudulent Emails

This document provides information to users of IATA products and services (e.g. airlines, agents, other companies and individuals) so that they may avoid becoming victims of email fraud attempts. Please read this information carefully and share it with your colleagues.

Contents

Email Fraud Techniques 2
Examples of Fraudulent emails 4
Examples of fake invoices/bank notices/letters 7
Report a possible fraud 12
Learn how to protect your company 13
Frequently Asked Questions 15
General Security Guidelines 17

If you have any questions concerning this document, kindly send your queries to information.security@iata.org
Email Fraud Techniques

Many types of fraud exist, and email is an inexpensive and popular method for distributing fraudulent messages to potential victims. Approximately 90% of all email sent worldwide are spam, spoof and phishing.

Some of the most common fraudulent messages are non-monetary hoaxes or non-monetary chain mail. Treat these as you would with any other spam. However, if you receive an email message that appears to involve payments, or asks for personal information such as login ID’s or passwords, do not respond.

Do not give out private information, reply to text messages, download or open attachments or click on any links in emails you are not sure they are genuine.

Methods employed generally include elements of the following:

1. **The fraudster contacts users under a false name**, sometimes similar or identical to the names of IATA officials, seeking payment for products or services and/or claiming payments for outstanding amounts due.

Recent examples of fraudulent email accounts:

Please refer to our [website](#) for an updated list of the current most used fraudulent email address.
1. **The fraudster uses a technique which allows the name of the true sender of an email to be masked**, so that the email appears to have been sent from a valid IATA address like invoice@iata.org. In such cases, the fraudster asks the recipient to ‘reply-to’ another email address, such as a “…..@gmail.com”.

2. **The fraudster uses forged documents** bearing the official IATA logo, most likely copied from IATA website. These can appear to be legitimate invoices.

3. **The fraudster’s email may suggest clicking on a link.** After clicking on the link, the user is taken to a fake IATA website that requests your login details, the purpose of which is to steal your login credentials.

4. **Fraudsters call IATA customers and impersonate IATA staff.** This attempt at fraud is increasing. Although telephone numbers may seem correct based on location, please remember that with Internet phones, the fraudster can call from anywhere.

   The names of IATA employees in email signatures have most likely been obtained when recipients of a first fraudulent email have provided copies of previous correspondence with IATA. **In some cases, the phone numbers in email signatures have been changed to invalid numbers**, a technique most likely designed to prevent the recipient from contacting the sender by phone. At other times, a working number is provided, but the person answering is not an IATA employee.

   **Legitimate emails from IATA end in the ‘@iata.org’ domain.** For different purposes IATA also uses @info.iata.org, @training.iata.org @updates.iata.org, @services.iata.org and @bsplink.iata.org.

   Please remember that although IATA is actively working to implement anti-spoofing measures, **any email address can be spoofed** to look like another. If in doubt, please contact information security.
Examples of fraudulent emails

Typically, the first contact is a generic email designed to elicit a response from the recipient. If the recipient engages with the fraudsters, they then provide a more detailed request, using language most likely copied from our website.

Being able to recognize fraudulent emails can help prevent you from becoming a victim. Following are examples of some emails received by users of IATA products and services.

Example No. 1

From: IATA Invoiceing [mailto: invoices@iata.org] [reply to: iata.acc@gmail.com]
Sent: Sunday, June 12, 2016 6:11 AM
To: undisclosed-recipients:
Subject: IATA Invoice Issue

Dear Sir,

Your company still have IATA invoices that are overdue for payment, Kindly check your records and get back to us as soon as possible if payment has been made we would appreciate if you could send us a copy of the Invoice... Failure to do so may lead to sanctions

Expecting your usual prompt co-operation

Best Regards,

Karen Welsh

Accounts /Invoicing
International Air Transport Association
IATA Head Office.
Example No.2

From: International Air Transport Association <payments@iatacollections.com>
Sent: Mon, 6 Jun 2016 11:44:55 -0400
Subject: IATA OUTSTANDING INVOICES!!

IATA OUTSTANDING INVOICE

Our Record shows that you have IATA invoices that are due for payment, kindly check your records and get back to us as soon as possible for payment, as failure to do so may lead to sanctions. Please note there is an update in vendor account information, we request you contact us for resolution of this due(s).

We expect your usual prompt cooperation.

Best Regards,
--

Lora Gomez
Accounts/Invoicing
Email: payments@iatacollections.com

International Air Transport Association
800 Place Victoria, PO Box 113
Montreal - H4Z 1M1
Quebec - Canada

Sometimes, these emails are accompanied by a fraudulent invoice. The invoice appears at times to be based on a genuine IATA or Strategic Partner invoice.

Fraudsters have been able to make these look reasonably authentic as some recipients of the first email have queried the existence of outstanding amounts and provided the fraudster with a copy of a genuine invoice that had already been paid, this provides the fraudster with an appropriate invoice style and content.

Fraudulent invoices in the past have included charges relating to IATA Ground Handling Council membership fees, designator fees, discounted Strategic Partnership memberships, and prefix code retainer/administration fees.
The fraudster indicates in the emails or on the invoices that new payment arrangements are in force and that the payment requested (or simply future payments where the approach is generic in style) should be made to a new bank account.

Bank accounts with the following financial institutions have been used by fraudsters recently; however, if a bank is not listed here, it does not necessarily mean that is legitimate from IATA account.

**Indonesia**: BNI, Bank BTN, Bank Mandari, BCA


**India**: ICICI Bank.

**Poland**: PKO Bank, Bank Pekao.

**Hungary**: K&H Bank, Oberbank, Raiffeisen.

**Belgium**: Belfius Bank.

**Czech Republic**: Unicredit Bank CZK.

**Finland**: Paijat- Hameen Osuuspankki Bank.


**Germany**: Postbank Hamburg, Sparkasse Lueneburg.

**Italy**: Unicredit.

**Malaysia**: OCBC
Examples of fake invoices/bank notices/letters/ certificates

It is important to note that without the efforts of IATA customers, we would not know what fraudulent accounts have been opened. If you receive ‘new’ banking details in any form, please forward them to Information Security whether or not you recognize it to be fraud. Allowing IATA to notify the bank and save others from becoming victims of fraud.

Examples of fraudulent invoices with false banking information:

![IATA Invoice Example]

*ANNUAL MEMBERSHIP FEE /CASS*
International Airline Training Fund

![Authorized Signature]

**PAYMENT REMARKS:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Period</th>
<th>Amount</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANNUAL MEMBERSHIP FEE</td>
<td>08.11.14</td>
<td>US$4,500.00</td>
<td>FIXED FEES</td>
</tr>
<tr>
<td>CASS SYSTEM FEES</td>
<td>08.11.15</td>
<td>US$1,500</td>
<td><strong>Contribution</strong></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>US$6,000.00</td>
<td></td>
</tr>
</tbody>
</table>

**PAYMENT CODE:** TRANSFER

**CURRENCY:** USD

**Authorized**

---

7
INTERNATIONAL AIR TRANSPORT ASSOCIATION
IATA Indonesia, Summitmas II, 17th Floor,
Jl. Jend. Sudirman Kav. 61-62, Jakarta - 12190
GST Number 107510570R10001

CHANGE OF ACCOUNT DETAILS

This is to inform you that there has been a change in our vendor account details for all IATA payment, Kindly check below for our new vendor IATA Indonesia Bank Account details and update your system for future payment.

BANK NAME : Bank Bni
ACCOUNT NUMBER : 0359898765
ACCOUNT NAME : IATA
BANK ADDRESS : Bank Bni branch imam bonjol tangerang Indonesia
SWIFT CODE : BNINIDJA
Fraudulent letters are issued to obtain payments or information from any IATA stakeholder. These letters are sent from fake IATA email addresses and come as attachments in PDF format.

Examples of fraudulent letters:

Dear Sir/Madam,

International Air Transport Association (IATA) is currently working on an exercise to reconcile actual account’s (Depts) totals with those that are noted on our Accounting system.

As a member of IATA; I have been tasked with making contact with a number of depts to collect and reconcile data.

I would therefore be grateful if you could revert back by return Email with totals owned by you as at 31 July 2015.

This exercise shall in no way hamper the usual workings of our finance department, but give us an independent verification of totals.

Please do not hesitate to contact the undersigned if you have any queries.

Yours Faithfully,

Guy Brazeau
Director
IATA Consulting
Tel: +1-514-874-1329, ext.
Mob: +1-514-402-0202
brazeau@iataconsult.org
There is no such prize; in fact fraudsters would request your personal information in order to follow up with the prize. Allowing them to misuse your information and identity.
Example of a fraudulent prize certificate:

![Image of a fraudulent prize certificate](image)

As in the last example, the prize is fake and fraudsters would request your personal information in order to follow up with the prize. Allowing them to misuse your information and identity.

**Fraudulent emails may also include a link that takes the user to a spoofed (fake) IATA website.** The purpose of spoofing an IATA website is to mislead the user into believing he is logging on to a legitimate IATA website.

Once the login details are captured, the fraudster can then use the information to login as the user to obtain billing information that will add authenticity to the fraudulent email attempts. In the case of finance systems and billing, you should always manually navigate to an official website, instead of "linking" to it by clicking a link from an unsolicited email.

*Remember that although IATA is actively working to implement anti-spoofing measures, any email address can be spoofed to look like another. If in doubt, please contact: Information Security*
Report a Possible Fraud

If you receive a suspicious or potentially fraudulent email, please report the relevant information using the guidance below:

When reporting such messages, it is important to copy and paste the entire email, including the header information.

To display full message headers:

Open the mail message.

- Outlook 2013: Open the mail in question and select ‘file’. Info > Properties. Your message headers are displayed
- Outlook 2007: double-click the message so that it opens in its own window. In the Options group, click the dialog box launcher (Small Square with an arrow).

To insert the headers into an email message:

Copy-paste the headers into a new email to: information.security@iata.org. Alternatively, once the email is open; it can be saved and then sent as an attachment directly to information security.

Please also forward any attachments that you receive from a fraudster: When we receive this information, it allows us to notify banks to close accounts immediately. Your actions can help save other IATA customers from being victims of fraud.

If you believe you are a victim of email fraud attempt, we recommend that you also contact your local law enforcement authority immediately. Action Fraud UK, IC3 in the United States and the Canadian Anti-Fraud Centre. For other jurisdiction please contact Information Security.
Learn How to protect your company from fraud

All organizations are vulnerable to fraud, especially if elements of the following apply:

1. **Belief that fraud doesn't affect your organization.** In truth, businesses around the world lose millions each year to frauds. Many organizations aren't even aware that they have fallen victim to fraud.

2. **Organization does not have set procedures in place** to authorize purchases, pay invoices and review expenditures.

3. **Personnel are distracted** when they pay invoices such that fraudulent emails and invoices escape their notice.

4. **Personnel do not have time to verify** the source of the email requesting payment. To resolve the matter, the invoice is paid out of convenience without further investigation.

5. **Organization experiences regular staffing changes related to high turnover,** part-time or volunteer staff which increases the risk of falling victim to a fraud.

6. **Personnel recognize the name** and logo of IATA from having paid similar invoices in the past. As a result, they might not review transactions or invoice details before making a payment.

7. **Organization does not report the fraud** because personnel are either embarrassed or ashamed. Law enforcement agencies depend on organizations that have fallen victim to come forward and report fraudulent activity. IATA may be able to assist, please do not hesitate to contact us.

**Here are other points IATA suggests you do to protect your organization from email fraud:**

1. **Don’t judge reliability** by look and content. Email messages can come from many sources and with the help of today’s technology a fraudster can make an email and invoices appear to be coming from a reputable source.

2. **Be wary of requests** to “update” bank account information or to pay overdue invoices as you may be providing criminals with the information they need to gain access to others in your organization or to defraud third parties.
3 **Implement a policy** of checking, and having independent approval of, any changes to existing, or setting up any new, payee bank account details.

4 **Assign a limited number** of employees to make purchases. Make sure that employees with financial signing authority understand what responsibilities are tied to signing their names on invoices and purchase orders.

5 Do not click on attachments to or links in fraudulent emails as they might contain **viruses** that can harm your internal systems. Instead, save the entire email and send it to information security.

6 **Double check the URL of websites and links.** Companies always use clear URLs like [http://www.iata.org/Pages/fraudulent-emails-websites.aspx?tab=1](http://www.iata.org/Pages/fraudulent-emails-websites.aspx?tab=1) Scam sites and links usually have long addresses using special characters like =j&q=&esrc=s&source=web&”

7 **Talk to your staff and colleagues about fraud.** Decide how your organization will handle situations involving employees coming forward to report losses.

8 **Be wary of collection calls from ‘IATA’ staff.** Due to the availability of worldwide telephone numbers, fraudsters are now purchasing Canadian and other numbers in order to appear to be calling from an IATA office. If you receive such a call, usually followed by an emailed invoice, contact information security for verification.

9 **Fraudulent messages can look like they’re from IATA,** but on closer inspection are from a public email account. For example, iatabsp1@gmail.com is not a genuine IATA email address.

10 Look for **grammar and spelling mistakes.** Scam emails are often electronically translated from different languages, resulting in spelling errors.

11 **If you receive a fraudulent email,** IATA suggests that you block the sender using your email client and delete the email in order to stop further attempts from the same email address.
Frequently asked questions

What addresses does IATA use to send emails?
IATA uses many addresses to send emails to its customers. All IATA emails typically end in ‘@iata.org.’ Though there are subdomains like ‘@info.iata.org’, ‘@updates.iata.org’ and ‘@bsplink.iata.org’ are other domains used for different purposes. Please be aware that fraudsters using phishing methods to make an email address appear to end in “@iata.org”, but the reply address will always be different. If you are unsure whether an email from IATA is genuine or not please do not hesitate to contact Information Security information.security@iata.org.

I just realized I have paid a fraudulent invoice, what do I do?
We advise that you contact your bank and notify them to cancel or recall the payment. Also inform your local authorities and raise a complaint at their office or via their website.

What can I do to protect myself?

- Immediately contact Information Security when you receive emails/invoices that appear suspicious or fraudulent.
  - Do not panic, often these fraudsters will use threatening language in order to get you to pay into their account as soon as possible. They may even call your office and pose as an IATA employee. First check with Information Security to see whether the suspicious email/call you received is valid or not.

- Distribute the information about fraud tactics around your office.
  - You can give our fraud warning to your company’s internal communication to circulate and also let your colleagues know the tactics that are being used by fraudsters. The more people that are made aware of fraudulent attacks, the less susceptible they are to fraudulent attacks.

- Pass information regarding fraud prevention to new employees
  - New employees can easily fall prey to fraudulent attacks because most are unaware of how to identify and deal with fraudulent attacks. If you are leaving your current position in your organization, we advise that you pass any information you have to the new employee if possible. If circumstances do not permit, please advise your HR department to inform your replacement about the fraudulent emails and invoices.
Please visit IATA’s website for more information about most used fraudulent emails, phishing attacks and tactics used by fraudsters.

**I received a suspicious email, but it is from an IATA employee**

Fraudsters have been known to use the names of real IATA employees in order to make their fraudulent email appear legitimate. Please forward all suspicious emails to information.security@iata.org
General Security Guidelines

Change your password regularly.
This will prevent people from having access to your account.

Avoid using the same password for multiple accounts (your personal email, work email, online forum etc.)
If one account is compromised, then your work email could be as well.

Do not open attachments from unknown sources and do not run programs that are attached in emails that are unknown to you.
These may contain malware that may give fraudsters access to your computer and secure emails.

Do not play games (especially online games) on your work computer. Online games are frequently attacked by hackers and cheaters who can gain access to your computer through the games security loophole.

If you do not need Java or Flash, disable them from your browser.
Ask you IT support group if you are unsure.

Ensure that your anti-virus is up to date and that your firewall is active. This helps protect you from viruses or malware such as key loggers that try to obtain your password data.

If you connect to an open/public Wi-Fi network. Attackers can easily intercept/sniff your network traffic, meaning that they could see whenever you attempt to log in to your email or make an online payment and gain your credentials. Therefore, IATA suggests you to be very cautious whenever you connect to a network that is open to everyone.

Close the browser after logging out. You not only need to log out of your email when you are done, but you also need to make sure to close the browser window completely. It compromises your email security.

Use a spam filter on email servers: Teach your users how to identify junk mail even if it's from a trusted source.
What security measures does IATA have in place to prevent fraud?

IATA uses a sophisticated email-validation system (DMARC) to detect, combat and prevent phishing attacks. DMARC combines two authentication mechanisms, Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) that allow email users to screen the legitimacy of internet domains.