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

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.

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

Several attempts have been made to obtain payments from users of IATA products and services. The most common technique is through the use of fraudulent emails, with or without fake invoices attached. Additionally, some attachments to fraudulent emails have been found to contain viruses.

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.

2. **The fraudster uses an email address resembling an IATA** email address but using different domain names.

   Recent examples:

any e-mails from @iata-account.org	**any e-mails from @iataworld-wide.org**
any e-mails from @iata-invoices.org	**any e-mails from @iatabillpayments.org**
any e-mails from @iatafinances.org	**any e-mails from @gmail.com**
any e-mails from @iata-finance.org	**any e-mails from @yahoo.com**
any e-mails from @iata-accounting.org	**any e-mails from @outlook.com**
any e-mails from @iataacademy.org	**any e-mails from @iata-receivable.org**
any e-mails from @iatamembers.org	**any e-mails from @iatabsp.org**
any e-mails from @iatagsa.org	**any e-mails from @bsplink.co.za**

   * Please refer to our website for an updated list of the current most used fraudulent email addresses.

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 finance@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 our 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. If you get a suspicious bill collection call, please note the number and contact information.security@iata.org .

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 tactic 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 rare mass mailing campaigns, legitimate emails may end in '@info.iata.org' or '@updates.iata.org'. Note that these still end in the 'iata.org' domain.

Situation 1: Fraudster calling IATA customer

Company C received a fraudulent email offering a discounted Strategic Partnership membership renewal for the following year. After responding to the fraudster with a request to proceed, the Company C received an email with a fake IATA invoice attached. The invoice included bank account details in Indonesia. The email requested that Company C send confirmation of payment via email.

Fortunately, Company C was skeptical about the new banking instructions and contacted IATA directly to verify rather than responding to the fraudster. IATA was able to warn Company C that the email and invoice were fraudulent. However, Company C received calls from individuals purporting to be from IATA, asking for payment status. Because IATA was able to warn Company C, these calls were ignored and the fraudster did not receive payment.

*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

-----Mensagem original-----
De: International Air Transport Association [mailto:noreply@iata.org]
Enviada em: quinta-feira, 14 de agosto de 2014 01:24
Assunto: IATA OUTSTANDING INVOICE!!!

Fraudsters "spoofing" genuine IATA address.

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 here asap for the new Vendor account information before your next payment.

Reference made to payment into a different account.

Expecting your usual prompt cooperation.

Best Regards,

Lora Gomez
Accounts/Invoicing
iatabillpay@accountant.com

Not a genuine IATA address or domain. An attempt to trick customers into thinking IATA uses accountant.com to settle bills, IATA does not use this service or domain.

International Air Transport Association
IATA Head Office, 800 Place Victoria,
P.O. Box 113 Montreal, Quebec - H4Z 1M1 Canada

This electronic mail may contain privileged or confidential information. It is intended only for the person to whom it is addressed. Any unauthorized disclosure, distribution or reproduction is strictly prohibited. If you have received this e-mail by error, please delete it immediately and notify the sender by returning an e-mail at the above.

This email is not a spam. To remove yourself from future mailings of this nature, click here Unscribe

Example No.2

From: INTERNATIONAL AIR TRANSPORT ASSOCIATION
[mailto:iata.paymentdesk@gmail.com]
Sent: Wednesday, August 06, 2014 8:25 AM
Subject: IATA PENDING PAYMENT

Dear Accounts,
Kindly confirm if you received our last IATA invoice.
Please note,due to ongoing audit in our account,there is a change in our banking details,kindly inform us when your company would be making payment so we can update you with our new account information.Expecting your prompt cooperation. Regards,
Diane Rinehart
Accounts/Invoicing
International Air Transport Association
IATA Head Office, 800 Place Victoria,
P.O. Box 113 Montreal, Quebec - H4Z 1M1 Canada

Some fraudsters use an email account such as Gmail.

Some emails will refer to a "problem" with the bank or your account and urge you to make payments to a new account. We will never notify you of a banking problem through an unsolicited email.

There is often a sense of urgency in the email encouraging you to respond immediately or face a sanction or suspension. If you actually have a valid IATA invoice due, you can verify this by logging a query with Customer Services: http://www.iata.org/customer-portal/Pages/index.aspx

Example No.3

De: International Air Transport Association [mailto:iatabillpay@accountant.com]
Enviada em: quinta-feira, 14 de agosto de 2014 12:41
Assunto: Re: RES: IATA OUTSTANDING INVOICE!!!

Dear xxxxx,

Find in attached file outstanding Invoice and Confirming the account you will be making payment, kindly acknowledge the receipt of this Message as soon as you recieve it. Do send us a Confirmation Slip once payment is made to our approved account in the INVOICE. Your Quick response will be appreciated as you have limited time before **15.AUG.14** to pay this outstanding invoice before it's overdue for payment.

We the **International Air Transports Association** advise as follows:

Annual Membership fee is a fee remitted annually to the **International Air Transport Association** for being a member of our Organisation.

Certificate Fee is a fee for the membership accreditation certificate, as a member of the **International Air Transport Association**, with the Certificate, you can be getting work referrals coming to **Brazil,** this will also benefit your company.

Adjustment for credits is a fee that allows your company to owe the **International Air Transport Association** for a maximum of 1-year when your company is having financial crisis or when your company needs loan from us with this payments you will get it within 5working days.

We advise payment should be remitted to us

Thanks for your co-operation.

Best Regards

Lora Gomez
IATA Finance Disbursement Manager
Phone:+1 647-795-7398
Email- iatabillpay@accountant.com

International Air Transport Association
800, Place Victoria, P.O. Box 113
Montréal, Québec, Canada H4Z 1M1

Tries to appear credible by explaining fraudulent charges in the invoice

Not a valid IATA email address or domain

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. Please see examples here: Examples of fake invoices/bank notices

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, but please note that even if a bank is not listed here, it does not necessarily mean that a 'new' bank account is a legitimate IATA account:

Canada: CIBC, Royal Bank of Canada, TD Canada Trust

Cyprus: Hellenic Bank; Piraeus Bank

Hong Kong: Hang Seng Bank

India: State Bank of India

Indonesia: ANZ Bank Panin; Bank BNI; Bank BRI; Bank of India in Indonesia; Bank Mandiri; Bank UOB; CIMB Niaga Bank; Permata Bank; Bank Danamon

Ireland: AIB Bank

Nigeria: FCMB;

Norway: DNB Bank; Nordea Bank Norge ASA

Singapore: ANZ Bank; DBS Bank; Standard Chartered Bank

Switzerland: Centrum Bank Ltd; Hinduja Bank Switzerland Ltd

Thailand: Bank of Ayudhya Public Company Ltd, BANGKOK BANK PUBLIC COMPANY LIMITED BANK, KasikornThai Bank PCL

Ukraine: PJSC IDEA Bank, PJSC VTB

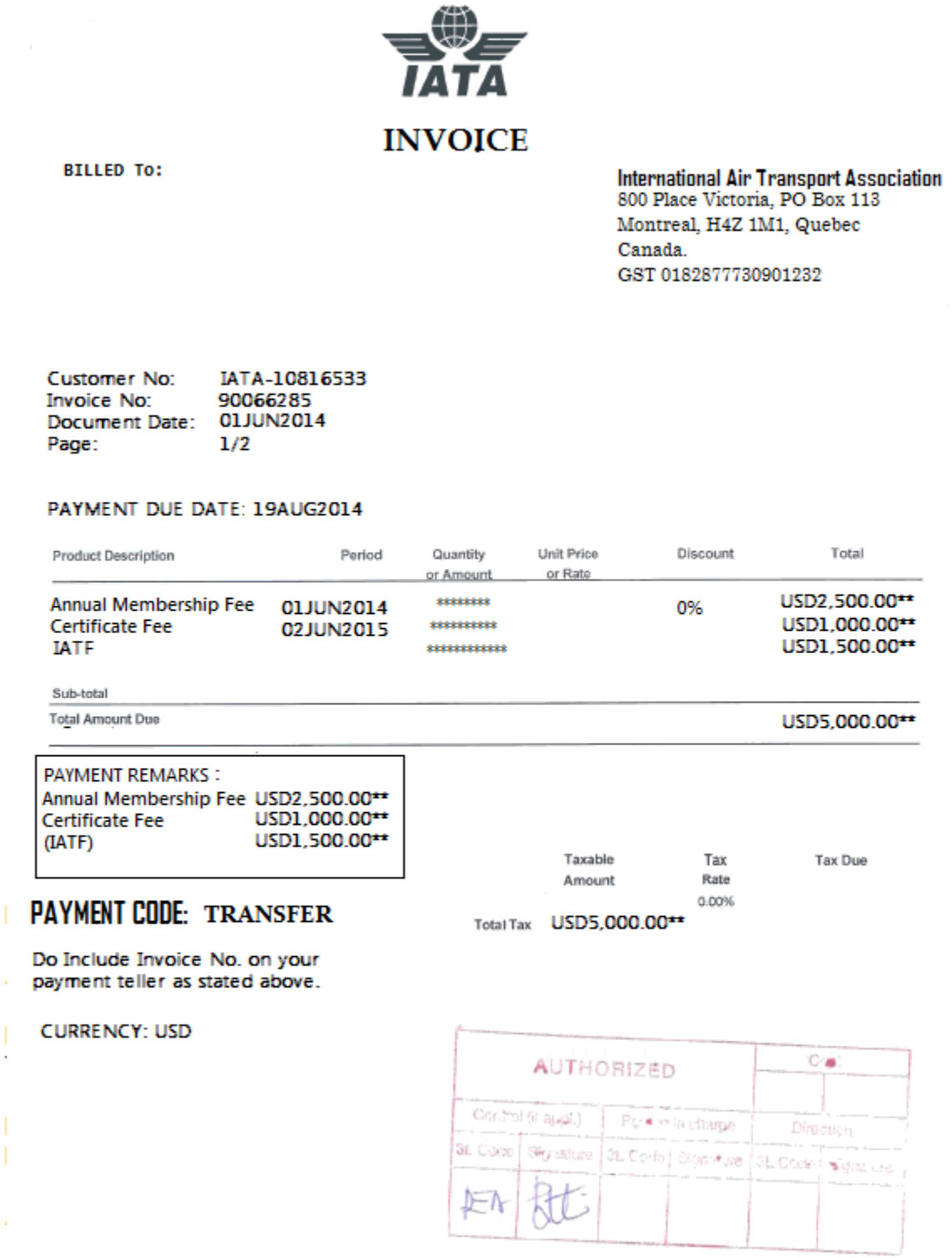
United Kingdom: Abbey Bank; Barclays; Halifax Bank; HSBC; Lloyds TSB; MetroBank Plc; NatWest; Royal Bank of Scotland; Santander Bank

United States: Bank of America; Chase Bank; TD Bank; First Financial Credit Union; First Keystone; PNC Bank; Prosperity Bank; Smart Financial Credit Union; SunTrust; US Bank; Wells Fargo

Examples of fake invoices/bank notices

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. **This will allow us to notify the bank promptly, and may even save others from becoming victims.**

Examples of fraudulent invoices with false banking information:



IATA

INVOICE

BILLED To:

International Air Transport Association
800 Place Victoria, PO Box 113
Montreal, H4Z 1M1, Quebec
Canada.
GST 0182877730901232

Customer No: IATA-10816533
Invoice No: 90066285
Document Date: 01JUN2014
Page: 1/2

PAYMENT DUE DATE: 19AUG2014

Product Description	Period	Quantity or Amount	Unit Price or Rate	Discount	Total
Annual Membership Fee	01JUN2014	********		0%	USD2,500.00**
Certificate Fee	02JUN2015	**********			USD1,000.00**
IATF		**********			USD1,500.00**
Sub-total					
Total Amount Due					USD5,000.00**

PAYMENT REMARKS :
Annual Membership Fee USD2,500.00**
Certificate Fee USD1,000.00**
(IATF) USD1,500.00**

	Taxable Amount	Tax Rate	Tax Due
		0.00%	
Total Tax	USD5,000.00**		

PAYMENT CODE: TRANSFER

Do Include Invoice No. on your payment teller as stated above.

CURRENCY: USD

AUTHORIZED

IATA RECEIVABLE DEPARTMENT

Attn:

International Air Transport Association
33, Route de l'Aéroport
1215 Genève 15 Aéroport,
Switzerland.
GST 0182877730901232

AUTHORISED BANKING DETAILS FOR REMITTANCE OF INVOICE #90066285

BANK NAME: SANTANDER UK PLC

BANK ADDRESS: 21 PRESCOT STREET, LONDON, UNITED KINGDOM.

ACCOUNT NAME: IATA

SORT CODE: 09 01 27 (IATA APPROVED)

IBAN: GB57 ABBY 0901 2738 3094 56

SWIFT CODE/BIC: ABBY GB2L ANB

Signed:
Lora Gomez
IATA Finance Disbursement Manager
Tel: +1 647 795 7398
iatabillpay@account.com

APPROVED
BRIAN THOMAS
Director of Finance

IATA RECEIVABLE DEPARTMENT

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.

If you have, or even believe you may have inadvertently responded to and/or activated any link or attachment within a fraudulent email, please contact Information Security with the corresponding details.

For further insight into the techniques deployed by fraudsters, please read the tnooz.com article for a further example. Please note that although this article indicates that only the domain 'iata.org' is legitimate, for rare mass mailing campaigns, legitimate emails may end in '@info.iata.org' or '@updates.iata.org'.

Situation 2: Fraudulent invoice

Company A received an email from a Gmail email address, but apparently from IATA's Director General and CEO, advising them that they were indebted to IATA. It stated that, if they failed to take action, IATA's 'international debt collectors' would visit the company.

The company did not consider the email to be suspicious, even though it was not addressed to them specifically (it had been sent to the Operations Manager's email address listed on the company's website), the language used was threatening, it came from a "gmail" address, and was apparently from the CEO of IATA.

Company A was coincidentally about to renew their membership of the IATA Ground Handling Council (IGHC) and responded to the fraudsters, asking if it related to that. The fraudsters confirmed that it did and sent the company an invoice. The invoice bore the IATA logo (most likely obtained from the internet). The email from the fraudsters referred to a change in bank account and asked the company to make the payment to the account detailed on the invoice. This bank account was in Cyprus.

The company made the payment to the fraudsters' bank account.

When the company received a reminder from IATA about their outstanding IGHC renewal fees, they realized that they had been defrauded.

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.*

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.

- In Outlook 2010: click the message so that it opens in its own window. In the menu above click File, then click Info and then the Properties box.
- In 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:

Select all the headers by clicking and dragging the cursor from the top left corner to the bottom right corner of the header text. Press Ctrl+c to copy the headers to the Clipboard. Create a new email message, click in its main text window, and press Ctrl+v to paste the headers into the 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 all offer assistance. For other jurisdictions please contact Information Security.

Legitimate emails from IATA end in the '@iata.org' domain. For rare mass mailing campaigns, legitimate emails may end in '@info.iata.org' or '@updates.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.*

Learn how to protect your company

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 things you can do today 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. **Review all invoices** and charges regularly.

3. **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.

4. **Implement a policy of checking, and having independent approval of, any changes to existing, or setting up any new, payee bank account details.**

5. **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.

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

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. **If you do receive a fraudulent email, we recommend that you block the sender using your email client in order to stop further attempts from the same email address.**

10. **If you are leaving the company or your current position**, we recommend you pass this document to your manager, and advice them to give this document to the new employee is aware of fraudulent techniques as well. We recommend adding this step to your Standard Operating Procedure.

PLEASE TAKE NOTE

Situation 3: Change in banking details

Company B received an email from someone who described themselves as a 'Customer Services Representative' informing them that they were indebted to IATA. It stated that, if they failed to take action, IATA's 'international debt collectors' would visit the company.

The email appeared to come from an '@iata.org' email address, but it asked the recipient to respond to another email address because IATA was experiencing problems with its '@iata.org' addresses.

The company did not consider the email to be suspicious, even though it was not addressed to them specifically (it had been sent via the contact us' link on the company's website), the language used was threatening, and it asked for a response to be sent to a non-'@iata.org' email address.

They did not think that they were in debt to IATA, so they responded to the fraudsters, asking for more information.

The fraudsters replied acknowledging that the company was not in fact in debt to IATA, and requested the company to inform them when their next payment was due, as IATA's banking details had changed, due to 'problems with the bank'. The fraudsters said that they would then send the company new banking details.

When the time came to make the next payment, the company notified the fraudsters, who provided account details for IATA's 'subsidiary' to whom payment was to be made.

The company subsequently made their next payment to the fraudster's bank account and did not question the fact that the new account was in a completely unrelated name, and based in China.

IATA's Accounts Receivable department contacted the company in due course to enquire about the payment of their now outstanding debt. The company informed IATA that they had already made the payment to the new bank account 'as requested', and provided confirmation of their payment. At this point, the company realized that they had been defrauded.

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.*

Frequently Asked Questions

How do I report fraudulent emails to IATA?

To report suspicious emails, please email Information Security at information.security@iata.org

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, which is used to send mass communication notification to IATA customers. 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. For more information on phishing attacks please click "here". 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 are sorry to learn that you have been a victim of fraud. We advise that you contact your bank and notify them to cancel or recall the payment. Also inform your local authorities and register a complaint at their office or via their website. We would like to kindly ask that you save the past corresponding emails with the fraudster and forward them as well as any fraudulent invoices to information.security@iata.org as well.

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 our website for more information about 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 you work email could be as well.

Do not open attachments from unknown sources and do not run programs that are attached in emails.

These may contain malware that may give fraudsters back 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, disable it from your browser.

Ask you IT support group if you are unsure.

When working from home, 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.

Do not connect to unsecure/unknown Wi-Fi networks when working outside the office.

Data that you transmit on these networks is seldom encrypted and can easily be seen by a third party.