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.

If you have any questions regarding the contents of this document, please send them to **information.security@iata.org.**

Contents

Email Fraud Techniques

Email, due to its inexpensive nature and ease of use, is a popular method for distributing fraudulent messages to potential victims. Approximately 90% of all emails sent worldwide consist of spam, spoofed messages, or phishing attempts.

Some of the most common fraudulent messages are non-monetary hoaxes or chain mail. You should treat these like any other spam messages – put them in your spam filter or simply delete.

Phishing emails can be more serious. These might ask for payment, for personal information, or even contain malicious links aimed at harvesting your personal information. These phishing attempts have been directed at users of IATA products and services, usually in an attempt to misdirect your payments to the fraudsters.

You can avoid being harmed by phishing if you follow these easy precautions:

- **Do not** click on any links in emails you are not sure are genuine.
- **Do not** download or open attachments unless you are sure they are genuine.
- **Do not** reply to text messages or emails requesting personal information, unless you can validate that these are from IATA.
- **Do not** give out any private information.
- **Delete** fraudulent emails and **block** the sender.

If you are not sure if an email is a genuine IATA communication, you can always check the IATA website (https://www.iata.org/Pages/fraudulent-emails-websites.aspx) or email information.security@iata.org.

Fraudulent emails in the last twelve months have often come from the following domains: @hotmail.com, @accountant.com, @gmail.com, @mail.com, @usa.com, accountinvoice-lata.org,@iataa.com, @iata-finance.org, @invoice-iata.org, @lata.org. **IATA does not communicate using these domains.** Check our website for an up-to-date list (https://www.iata.org/Pages/fraudulent-emails-websites.aspx).

Remember: we see new fraud email accounts every week, so this list is not exhaustive. Read on for more signs of fraudulent emails.

Fraudsters often use some or all of the following methods:

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

2) **The fraudster uses a technique which allows 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. This is called "**spoofing**." In such cases, the fraudster asks the recipient to click a link or 'reply-to' another email address, such as a Gmail address. If the email address changes when you click the reply button, this is a warning sign of potential fraud!

3) The fraudster may use the IATA logo and formatting in an attempt to replicate IATA documents. Some of these look close to IATA documents – but if there is a changed bank account or the expected reference number doesn't match, make sure to contact us for clarification or go straight to the Customer Portal.

4) The fraudster's email may suggest clicking on a link. After clicking on the link, you may be forced to download a file or be taken to a fake IATA website that requests your login details. The purpose of this is to steal your login credentials.

5) Fraudsters call IATA customers and impersonate IATA staff. Although telephone numbers may seem correct based on location, please remember that with Internet phones, the fraudster can call from anywhere. Caller ID can be spoofed in the same way email can!

Fraudulently used information, including logos, phone numbers, invoices, and names of IATA employees in email signatures, are often obtained when recipients of a fraudulent email provide copies of previous correspondence with IATA. You should avoid any communication with the fraudster or providing any details to them.

Fraudsters sometimes use phone numbers in email signatures. These may be invalid numbers, a working number that redirects to the fraudster, or even a genuine IATA number designed to make the email seem more legitimate.

EXAMPLE: 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.

Legitimate IATA emails end in the "**iata.org**" domain. IATA may also use the following:

- @consulting.iata.org
- @ebroadcast.iata.org
- @cnsc.us
- @iata.org.br
- @iatan.org
- @info.iata.org
- @training.iata.org
- @updates.iata.org

- @indp.iata.org
- @services.iata.org
- @bsplink.iata.org

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@iata.org**.

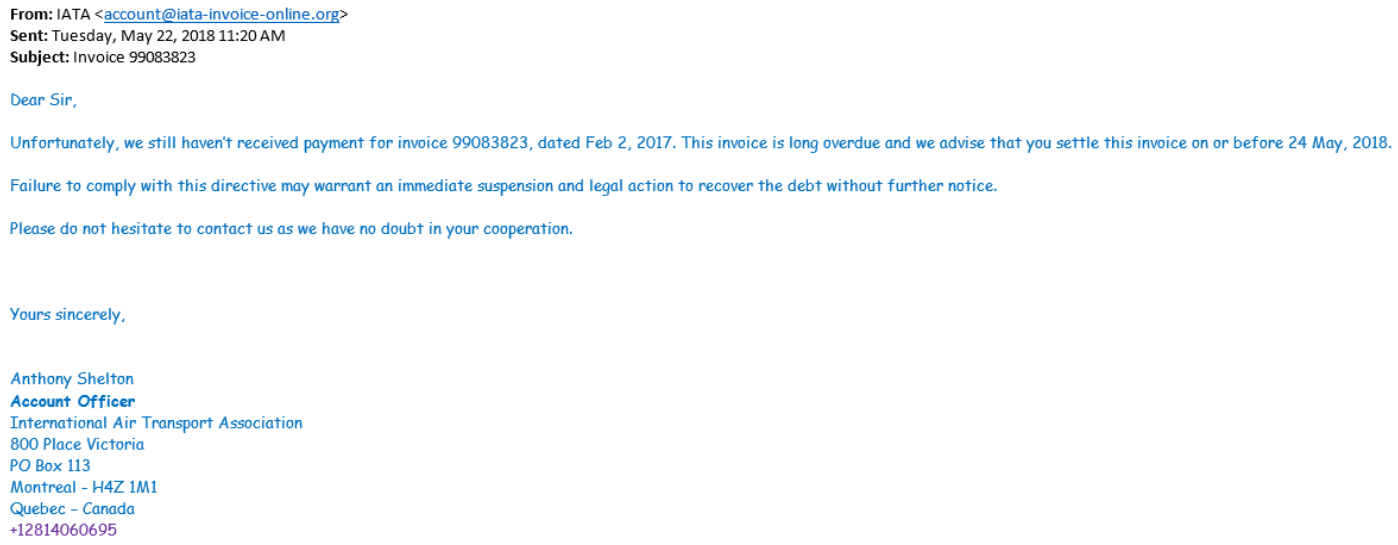
Examples of Fraudulent Emails

Fraudsters usually, but not always, follow a standard method. The first contact will be a generic email – often sent to dozens or hundreds of contacts – designed to elicit a response from you. It may say that your invoices are overdue and tell you to check your records, but won't mention a specific invoice or amount.

If you respond to the first email, they may send a more detailed request. This request may use language copied from our website.

Sometimes phishing and fraud emails will be targeted specifically to your organization after careful research by the fraudster. These fakes can be hard to spot. Your organization should have internal controls to verify payments before they are made.

Example #1



From: IATA <account@iata-invoice-online.org>
Sent: Tuesday, May 22, 2018 11:20 AM
Subject: Invoice 99083823

Dear Sir,

Unfortunately, we still haven't received payment for invoice 99083823, dated Feb 2, 2017. This invoice is long overdue and we advise that you settle this invoice on or before 24 May, 2018.

Failure to comply with this directive may warrant an immediate suspension and legal action to recover the debt without further notice.

Please do not hesitate to contact us as we have no doubt in your cooperation.

Yours sincerely,

Anthony Shelton
Account Officer
International Air Transport Association
800 Place Victoria
PO Box 113
Montreal - H4Z 1M1
Quebec - Canada
+12814060695

The above example creates a **sense of urgency** by demanding payment right away. It makes a **threat** regarding what will happen if you fail to pay in a short timeframe. The address is in Montreal, but the area code on the phone number is for **Houston, Texas**.

Example #2

From: International Air Transport Association [mailto:testmail@sustc.edu.cn]
Sent: Saturday, May 12, 2018 5:24 PM
To: [redacted]
Subject: IATA CASS INVOICES [redacted]

Dear Sir,

Your company is indebted to IATAkindly check your system/records carefully for IATA CASS INVOICES from Janunry to April 2018 and failure to do so may lead to sanctions.Please note there is an update in bank account information,we request you contact us here asap for our new bank account information before your next payment.

Expecting your usual prompt cooperation.

Best Regards,
Mary Freedom
Head of Accounts
Email:account@accountinvoice-lata.org

This example notes that there is **updated bank account** information, to try and stop you paying into your usual IATA account. It requests that you **check your invoices** instead of giving you a specific list of invoices to pay or asking you to log into your Customer Portal account and handle things directly there. It is sent from a **different email address** than the reply email account listed in the signature.

In the above case, sometimes customers will respond with a list of their previous invoices, some of which may already have been legitimately paid to IATA. The fraudster will then make an excuse saying that payments have not been received and request that you pay into a new account.

Fraudsters are often able to make invoices look reasonably authentic. **Do not send your invoices** if you receive an email like the above – fraudsters use these to update their techniques and victimize other customers!

Fraudulent invoices in the past have included charges related to IATA Ground Handling Council fees, designator fees, discounted IATA Strategic Partnership memberships, and prefix code retainer or administration fees.

Example #3

-----Original Message-----
From: IATA ACCOUNTING accounts@invoice-iata.org <accounts@invoice-iata.org>
Sent: Wednesday, July 11, 2018 [redacted]
To: [redacted]
Subject: IATA INVOICE

Dear [redacted]

Kindly login into our website below with your email and password to down load IATA Invoice for next payment:

http://iata.org.verify.document.share.iata-investment.org/webstar.iatan.org/
WebStarExtranetWEB/

Kind Regards,

Afa Quliyeva

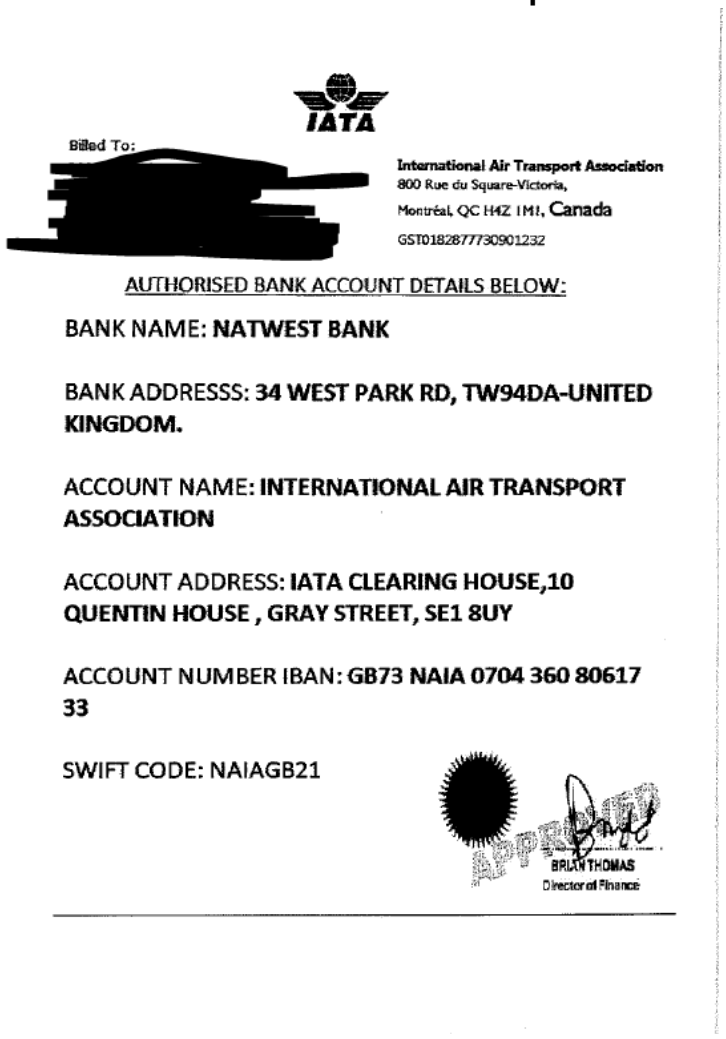
Sometimes fraudsters will tell you to **click on a link**. You may then be asked to enter a username and password, enter personal information, or download an invoice. **Do not click on the links** as they often contain malware that can seriously damage your computer. They may also seek to harvest your personal information for later use.

Examples of Fake Invoices, Bank Notices, and Letters

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 for verification. This allows IATA to notify the bank and save others from becoming victims of fraud.

If you have already paid to an account you suspect to be fraudulent, tell us immediately! We have managed to have fraudulent transactions reversed in the past where customers have informed us immediately.

Common Fraudulent Invoice Examples



IATA

Billed To:

[redacted]

International Air Transport Association
800 Rue du Square-Victoria,
Montréal, QC H4Z 1M1, Canada
GST0182877730901232

AUTHORISED BANK ACCOUNT DETAILS BELOW:

BANK NAME: **NATWEST BANK**

BANK ADDRESSS: **34 WEST PARK RD, TW94DA-UNITED KINGDOM.**

ACCOUNT NAME: **INTERNATIONAL AIR TRANSPORT ASSOCIATION**

ACCOUNT ADDRESS: **IATA CLEARING HOUSE,10 QUENTIN HOUSE , GRAY STREET, SE1 8UY**

ACCOUNT NUMBER IBAN: **GB73 NAIA 0704 360 80617 33**

SWIFT CODE: NAIAGB21

APPROVED

BRIAN THOMAS
Director of Finance

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: ROYAL BANK OF SCOTLAND PLC

BANK ADDRESS: CARTSDYKE AVE., GREENOCK, PA15 1EF, UNITED KINGDOM

BENEFICIARY NAME: IATA (IATA APPROVED)

SORT CODE: 83 15 31

IBAN: GB06 RBOS 8315 3116 2955 08

SWIFT CODE/BIC: RBOS GB2L XXX

Signed:
Lora Gomez
IATA Finance Disbursement Manager
Tel: +1 425 440 0124
invoicing@iatacass.org

APPROVED
BRIAN THOMAS
Director of Finance

IATA RECEIVABLE DEPARTMENT

IATA
Schaffhauserstrasse 104, P.O. Box 364,
CH-8152 Glattbrugg

[redacted]

Costumer No. IATA-[redacted]
Invoice Date: 01/18/2018

Please mention the invoice number when effecting your payment.

INVOICE No 18003356	Qty	Price	Amount in USD
Annual subscription for Corporate Logistics IATA Membership	**********	$2859.00	$2859.00
CASS SYSTEMS PERIOD 11.02.2017	**********	$4320.00	$4320.00
Cargo accreditation Certificate	**********	$3120.00	$3120.00
Cargo Control/ATFC Fees	**********	$2050.00	$2050.00
Total USD (US DOLLARS)			**USD $ 12,079.00**

Conditions of payment: 31st May 2018, without any bank expenses for us.

Kindly note, that your IATA Membership Fee 2017 still remains unpaid in our records. Your respective payment is highly appreciated.

Director Finance
Richard Rigby

IATA

Examples of Fraudulently-Used Banks

Accounts from the banks listed below have, among others, been used fraudulently to deceive IATA customers. This is a non-exhaustive sample of some accounts we have seen. Most banks, including the below, take their anti-fraud obligations seriously and cooperate quickly to close fraudulent accounts – but they need your reports to do so.

- United Kingdom
  - Barclay's, Lloyd's, National Westminster Bank (NatWest), HSBC, Yorkshire Bank, Halifax Bank, Metro Bank, Santander, Nationwide, TSB Bank, Royal Bank of Scotland
- United States
  - Chase, SunTrust, Bank of America, Wells Fargo, HSBC
- Indonesia
  - United Overseas Bank (Indonesia), Bank Central Asia
- Malaysia
  - Public Bank, Affin Bank
- Taiwan
  - Union Bank of Taiwan
- Netherlands
  - ABN-AMRO
- Spain
  - ING, Caixa
- Sweden
  - Swedbank
- Germany
  - Postbank Deutschland
- Austria
  - BAWAG PSK
- Ireland
  - Allied Irish Banks
- Turkey
  - Ziraat Bankası
- Slovenia
  - NBL Group
- Estonia
  - SEB Bank

Fraudulent letters have also been used in attempts to obtain payment or information from IATA stakeholders. These letters can be sent from fake email accounts and come as attachments in PDF format, but occasionally customers have received them by regular mail.

In these cases, fraudsters are attempting to obtain your personal information. They may use this in future scams, or may attempt to use your identity for criminal purposes.

These documents, or the emails they are sent in, 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 login details are captured, the fraudster can then use the information to login as the user. This could be used 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. Avoid clicking on any link from unsolicited emails.

Reporting Fraud

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

IATA analyzes emails to determine their origin so we can report them to host providers and registrars. To do this, we need access to the email headers. You can provide these to us in one of two ways:

- Send us the original email as an attachment. This will **not work** if the email has been forwarded to you by a colleague – it must be done by the original recipient.
- Extract the message headers and send them to us following the procedure below.
    - 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 them from the above location and paste the headers into a new email to: information.security@iata.org.
    - Alternatively, once the email is open, it can be saved and sent as an attachment directly to us.

Please also forward all attachments that you receive from a fraudster: This information gives us a full picture of the techniques fraudsters are using. It also helps us report active accounts to banks and relevant authorities. Your actions can help save others from becoming victims of fraud.

If you have **fallen victim** to a fraud attempt, don’t be embarrassed to report it. Send a report to us as well as to the sending bank, receiving bank, and your local law

enforcement immediately. If you are unsure of which law enforcement agency you should report to, contact Information Security and we will seek to assist you.

Protecting Your Company

It isn't just you. **All organizations are vulnerable to fraud**, especially if the following apply:

1) **You believe fraud doesn't impact you.** The truth is that businesses in every sector lose millions of dollars to fraud every year – and we are aware of cases from the tiniest, one-person operations to the largest multinational corporations. Many organizations might not even become aware of losses for months or years afterwards.

2) **The organization does not have controls or procedures** to validate or authorize purchases, pay invoices, or review expenditures. You should always have a secure process to handle payments, and require multiple levels of review and authorization if payment details change.

3) **Personnel with responsibility for review are overworked, distracted, or multitasking.** This makes it more likely for signs of fraud to go undetected. Make sure your personnel have the time and space to focus.

4) **Personnel do not have time to verify the source of the invoice**. The risk of a late payment is lower than the risk of a fraudulent payment. Never pay an invoice out of convenience without verifying it, especially if received through an unusual channel.

5) **The organization has high turnover**. Part-time, volunteer, or new staff may not have the experience to detect fraud. Have an expert nearby, or contact us for verification.

6) **The organization does not report fraud**, either due to shame, embarrassment, or a desire to move on quickly. Law enforcement agencies, banks, and IATA depend on you to report fraud so we can prevent it more easily. We may also be able to assist you with reversing transactions. **Not reporting fraud raises your future risk of falling victim again.**

Here are some quick tips to protect your organization:

1) **Don't judge reliability from appearances or content.** While many obvious fraud emails contain spelling mistakes, wrong invoice numbers, or badly-faked logos, some – especially targeted ones – can be very sophisticated. Modern technology makes email messages easy to fake!

2) **Don't trust requests to "update" bank account information** or to pay overdue invoices. Trying to confirm may result in your personal information being abused by a fraudster. Always verify changes by contacting IATA directly through other means, like emailing **information.security@iata.org**.

3) **Implement control policies**, including checking and independently approving changes to existing payment methods or bank information.

4) **Assign a limited number of employees** to make purchases or approve orders, and make sure they are trained and aware of their responsibilities in signing invoices and purchased orders.

5) **Do not open attachments or click links** in emails you suspect may be fraudulent. Instead, save the entire email and send it to **information.security@iata.org.**

6) **Double check the URLs of websites and links**. Companies usually use clear URLs, like http://www.iata.org/Pages/fraudulent-websites.aspx. Scam sites and links usually have long addresses using special characters (=j&q=&esrc=s&source=web&") or redirect to a different site than the one you were expecting.

7) **Talk to your staff about fraud**. Make sure they are aware of fraud techniques and unashamed to report losses and mistakes. If staff are scared to report mistakes, you may lose more money!

8) **Be wary of unsolicited calls or emails purporting to be from IATA staff.** Modern technology means that phone numbers can be spoofed or purchased with any area code imaginable. If you receive a call or emailed invoice, contact a trusted IATA number or email address – such as Information Security – for verification.

9) **Check the email address.** Is the section after the @ symbol a public domain such as accountant.com or gmail.com? When you hit reply, does the expected email address change? These are common signs of fraud. If you are not certain, check with IATA.

10) **Check for grammar and spelling errors.** This isn't a certain sign, but phishing emails often use poor English and may have been translated from another language. This results in spelling and grammatical errors.

If you receive a suspicious email, you should block the sender and delete the email in order to stop further attempts. Your IT team may wish to block the entire sending domain – the entire accountant.com domain, for example, may be safely blocked.

Frequently Asked Questions

Q: What addresses does IATA use to send emails?
A: IATA uses many legitimate email addresses to contact our customers and the public. Our emails typically end in @iata.org, but we have other subdomains such as @info.iata.org and @updates.iata.org which are used for other purposes. A full list is available above.

You should be aware that spoofing methods can make an email appear to end in @iata.org, even if it doesn't come from us. The reply email address will usually be different. If you are unsure, contact **information.security@iata.org.**

Q: What security measures does IATA use to prevent fraud?

A: IATA uses a sophisticated email validation system (DMARC) to detect, combat, and prevent phishing attacks. DMARC combines two security mechanisms called "Domain Keys Identified Mail" and "Sender Policy Framework." These allow email gateways to only accept emails complying with these two security controls.

Q: I have paid a fraudulent invoice. What do I do?

A: Contact your bank and ask them to cancel or recall the payment. Call your local law enforcement agency. Then email us, providing all the details of the payment, including sending and receiving banks. We are here to help.

Q: What can I do to protect myself?

A: Please see our list in the previous section. The most important individual steps you can take are:

- Don't panic if you receive a strange email – contact Information Security.
- Teach your employees about common fraud techniques.
- Check our website (https://www.iata.org/Pages/fraudulent-emails-websites.aspx) for information on the latest fraud activity.

Q: I received a suspicious email, but it is from an IATA employee.

A: The email may still be fake. Fraudsters have used the names of real IATA employees to make their emails seem more legitimate. **Forward suspicious emails to information.security@iata.org for verification.**

General Security Guidelines

1) **Change your password regularly.** If someone gains access to your account, this will prevent them from keeping it. Make sure your password is at least 10 characters long and complex (consider a minimum of one uppercase, one lowercase, one special character, and one number).

2) **Avoid using the same password for multiple accounts.** Sometimes passwords are hacked or leaked from unsecure sites. Lists are sometimes resold by fraudsters. This could lead to you losing access to all accounts. You may wish to consider using a password manager to help maintain unique and complex passwords.

3) **Do not open attachments or click on links from unknown sources, and never run a program from an unknown source.** These can contain malware that harms your computer, harvests your records, destroys your files, or asks for ransom payments. Programs called keyloggers can even record everything you type!

4) **Do not play online games on your work computer.** Security loopholes in these games can be used to attack your computer. If in doubt, check with your local IT team.

5) **Disable Java and Flash if you do not need them.** If in doubt, check with your local IT team.

6) **Keep your antivirus and firewall software updated.** This provides additional protection against malware.

7) **Avoid connecting to public or unsecured Wi-Fi networks.** Attackers can intercept network traffic, such as your email or online payment credentials. There are protective tools, such as VPNs, that can help counter this. Talk to your IT department about the best practices for you and your company.

8) **When done with your accounts, log out and close your browser.** This small step can ensure you are completely logged out.

9) **Use a spam filter, and don’t evade it.** Teach your users how to identify junk mail.

August 2018