

Please be Wary of Malicious Phish

OPSGROUP Team
24 June, 2021



There is a new threat to flight ops security, and it might not come from where you think it would.

The Hack Attack

We talked about the threats of airplanes and control towers being hacked before. But now we want to talk about cybersecurity.

Anyone who works for a big company has probably had to do their cybersecurity training at some point. If you haven't, here is an example. Answers at the bottom of the page.



Sebastian has no eyes or mouth. Or arms for that matter. But he does have a company laptop and needs to pick a password. Which one is going to be the most secure?

1. Sebastian1995
2. Password123
3. \$sdfh)sdg34d^(^(^SLF174h\$@fj))(_hslksd!!sdf5*\$:G68(^GS*%

The answer is 3. And no, it isn't my actual password.

The trouble is, the scams we have been seeing are getting more and more, well, *smart*.

The Nigerian Prince

The good old Nigerian Prince who wants to give you One Hundred Million Gazillion Dollars scam. **As old as the internet itself.**

How does it work? (And yes, these do still work. Apparently they **rake in over \$700,000 a year** from unwitting victims).

In a Kola nutshell, you receive an email from someone overseas (and there are different iterations of this now but it is always along the same lines) – a royal prince is **wanting to give you money**, or a disgustingly rich recluse of a distant uncle has passed away and mentioned you in their will.

Whichever they use, the trick is the same – they supposedly have money for you, and all you need to do is **provide your bank account details** and they will transfer it all over, for a small fee.

Only here is the catch (sorry to break it to you) – There is no Prince, there is no money, and **now they have your bank details** and maybe even a payment you have sent them.

This doesn't affect Flight Ops though?

No, it doesn't. Not really. Unless you count the **Nigerian Astronaut stuck in space** one.



They are reposing a lot of trust on you...

There is also the recent one which the NBAA warned about involving **Imposter CBP Agents** who call private residences and businesses and attempt to gain banking information.

And then there are the **fake websites** offering free tickets or special deals, and steal "passenger" information which they freely provide. [https://deltaairlines-flights.com] is not a legit website. Don't buy tickets from there.

The ones that we want to bring up though are **Phishing scams and Malware emails**.

So, what do you need to be on the look out for, and how do these even **impact Flight Ops and**

Security?

Be Wary of Malicious Phish

This is when an email is sent which looks legit. You open it, maybe it tells you there is an iTunes bill you need to pay. You wonder what you bought on iTunes, you can't remember, so **you open the attachment and BAM!**

Malware is sophisticated nowadays. It doesn't always just shut your computer down, or flash up a retro laughing skull icon. It might destroy data, it might steal data. It might install ransomware on your systems.



Great. And now the TRex has got out.

Hackers recently took hold of an oil pipeline in the USA.

The Colonial Pipeline supplies half of the east coast's fuel supply. Hackers managed to shut it off, probably via an email. The impact was **no fuel supply from Houston to New Jersey** and this affected all the airports along that route. It also led to **increased fuel prices and ongoing impacts** even after the fuel supply was re-established.



Cyber attacks are as common as physical ones

Phishing is a similar scam.

An email, or a phone call from a **“trusted source”** appears in your inbox and somehow cons you into giving login data, passwords, user info. Once access has been “granted” the hacker can do a lot of damage. From **stealing confidential information, to taking control of systems.**

I.T. Operator SITA which serves major Star Alliance airlines such as Lufthansa and Singapore suffered a **data breach in Q1 2021** with hackers gaining access to ticketing and baggage control systems which led to the information of thousands of passengers being stolen.

In 2020, major European regional airline EasyJet admitted an attack may have **compromised data of around 9 million passengers.** Several thousands had their credit and debit card details accessed.

What are we seeing at OPSGROUP?

We are seeing scammers getting more cunning, scams which are more targeted and ones which are **worryingly specific.**

First up, the **Nav Fees scam.** This one has been around for a while – we reported on it here. They send you an email, pretending to be from Eurocontrol or IATA or some government agency, with a new bank account to send your Nav Fees to. Pretty standard stuff. Fortunately, most of these emails are poorly written, and easy enough to identify as bogus – but that’s only if you are on your guard.

Then there’s the **charter quote email scam.** These have believable company names. Some of the names are even “real” people, so the email looks legitimate, and **all it does is ask for a quote.** So you open the email attachment and now they have you.

Thankfully, **OPSGROUP is not in the charter quote business** (and our email system is fairly good at spotting these now), but for some of you reading this, who do see real emails for quotes, this might pose a problem.



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe



Hi,

Could you advise a full charter price for the following attached details below :

[charter details.pdf](#)

Mit freundlichen Grüßen / Un cordial saludo / Best Regards

Sergio Rico Muñoz

Inside Sales Manager

Commercial Central Europe

(+49) 0 69

8088 3737

latamcargo.com

Please consider following Email accounts depending on the issue:

| | |
|--|---|
| cargosaleseur@latam.com | Quotes, Rates, Schedules, General Information, Allotment negotiation |
| grp_cargobookEUR@sac.latam.com | Update of Prebookings |
| CargoCareEU@latam.com | CCA, Incidents with Bookings of delivered cargo |

The Charter Quote scam

The more concerning ones come from very specific, and **very genuine aviation linked companies** such as 'Airbus'.

These are worrying because they are **so specific, so targeted**, that it is often hard to spot the real from the scam.

Microsoft put a warning out earlier in 2021 saying they are tracking this 'dynamic' campaign which is targeting the aerospace and travel sectors with **spear-phishing emails**. When the PDF in the email is opened it delivers RevengeRAT or AsyncRAT to your computer.

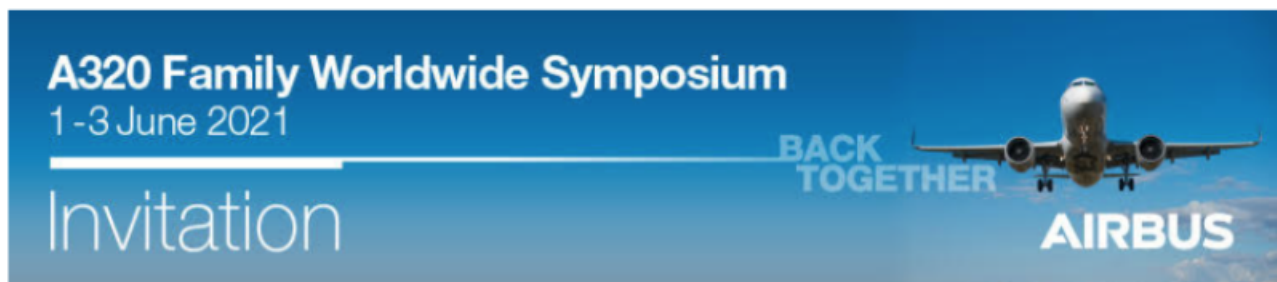
RATs it seems are the new worms. A Trojan is installed and user credentials, webcam info, statistics about the system are pilfered and pillaged.

Invitation to the A320 Family Worldwide Symposium

1 message

Airbus Invitation <non-reply@airbus.com>
Reply-To: non-reply@airbus.com

Thu, Apr 29, 2021 at 11:46 AM



Dear Customer,

Airbus is pleased to invite you to the A320 Family Symposium which will take place from Tuesday 1st to Thursday 3rd of June 2021.

The event will be an opportunity for us to provide you with an operational overview of what has been done to support the A320 fleet in 2020 through various virtual sessions & conferences. We will also focus on what are going to be the next steps in the support & development of the A320 Family.

The agenda thematics are focusing around the "Customer Support & Fleet efficiency" aspects and are not technically orientated.

Please find attached the global agenda of the event which is based on Toulouse (France) time (GMT+2).

 [Airbus Family Worldwide Symposium.pdf](#)

We kindly invite you to confirm your participation not later than Friday 28th of May by signing on the attached global agenda of the event and revert back immediately.

You will be provided with the connection details, once you have confirmed your participation.

We are looking forward to your participation in this event together paving a collaborative path for our future.

Joseph Sauras
Senior Director A320 Family Programme
Customer Services

Philippe Le Bigot
A320 Family Programme Manager
Customer Services

The information in this e-mail is confidential. The contents may not be disclosed or used by anyone other than the addressee. Access to this e-mail by anyone else is unauthorised. If you are not the intended recipient, please notify Airbus immediately and delete this e-mail.

The Airbus Symposium Scam is a known one

Your OPSGROUP Cybersecurity Assessment

1. If you receive an email from an unknown sender, or for something you haven't signed up to – should you open the attachment?

- Yes

- No
2. You receive an email or a call asking for details that involve passport info, bank details or anything else sensitive – should you share it?
- Yes
 - No
3. There is a Nigerian Prince/Princess who really wants to marry you and send you several million dollars – should you trust them?
- Yes
 - No

If you answered “Yes” to any of these questions, go back to the start of this article and read it again.

Fake Navigation fees are still a problem

Declan Selleck
24 June, 2021



It's a concern: instead of sending your Nav Fees payment to Eurocontrol, you've actually sent it to some guy sitting in his underpants in his mother's basement. And you're not going to get it back.

We've seen an increasing variety of scam emails, that at first glance look like they are from Eurocontrol – but aren't. Here's a good example from this week:

From: Alexandre Skonieczki
Date: June 15, 2020 at 7:29:41 AM EDT
Subject: open payment- eurocontrol
Reply-To: alexander.skonieczki@eurocontrolint.in

Dear Colleagues,

We have sent a couple of letters to you, but no response, could you please let us know the status of outstanding with respect to Air navigation and communication charges on review of your files, we discovered that these invoices in reference to your flight charges dated 15-02-2020 and 15-02-2020 for QPSIX (reference 05/044579/56/1906/01 and 05/044579/56/1907/01) are still in arrears, please kindly confirm the status of these invoices, that is let us know if payment has been made or not by providing a copy of the bank swift confirmation payment proof to enable us reconcile and update your account accordingly.

Note also that, the wire transfer and banking details have changed and the new payment instructions will be sent to you

prior to the next payment run, please advise accordingly, so that we can forward details promptly.

Thanks for your cooperation, we await your prompt advice.

Yours faithfully,

Alexandre Skonieczki

COLLECTION OF CHARGES
CRCO/CAT/ACCOUNTING
EUROCONTROL
Rue de la Fusee 96130
BELGIUM

You'd be forgiven for glancing over it and responding to request the details of 'their' new bank account. And that's where the problem begins - you'll get a new bank account, only it won't direct your money to Brussels.

IATA has the same issue:

IATA AGENT
To: Karen Welsh
IATA INVOICE

IA

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, 800 Place Victoria

Fortunately, most of these emails are poorly written, and easy enough to identify as bogus - but that's only if you are on your guard. The best solution is to simply be aware of the risk:

Eurocontrol

1. Look at the sender address: real emails come from **eurocontrol.int**. Fake ones look similar, but might be something like @eurocontrolinc.com or @eurocontrolint.in.
2. Most of the emails ask for a copy of an invoice or payment - be suspicious when you read that.
3. Be especially alert when the email mentions a **change in bank account**. Eurocontrol has no plans to change bank accounts any time soon.

4. Best advice: write to the real address: **r3.crco@eurocontrol.int** and ask for confirmation of any message, or call the Route Charges office on +32 2729 3838.
5. The most secure way to handle Eurocontrol charges and payments is through their CEFA portal.

IATA

1. Most recent fake addresses: *invoice@iatahelpdesk.org*, *payments@iataaccounting.org*
 2. Contact the real address: **information.security@iata.org**
-

The Air Charter Association have also warned that scammers have recently targeted business deals where operators charter out their aircraft to brokers. Similar to the fake IATA invoices scam, but more elaborate. Bottom line, if you're chartering out your aircraft — or if you're chartering one yourself — work with a reputable broker and triple-check all contact details (email addresses as well as phone numbers) and bank account details before pushing the button on any money transfers.

Even the mighty Japan Airlines fell victim to a targeted email scam back in 2017 which defrauded the company of JPY384 million yen – the equivalent of around USD \$3.4 million. The airline received a series of emails purporting to be from a U.S. financial services company that had been leasing aircraft to Japan Airlines. Not realising it was scam, JAL promptly paid the money into a Hong Kong bank account, as requested. It was only later discovered to be fraudulent, when the genuine U.S. company demanded payment!

Have you been the target of similar scams? Let us know! – and we'll add it to the list of dodgy email addresses and common scams.