Please be Wary of Malicious Phish

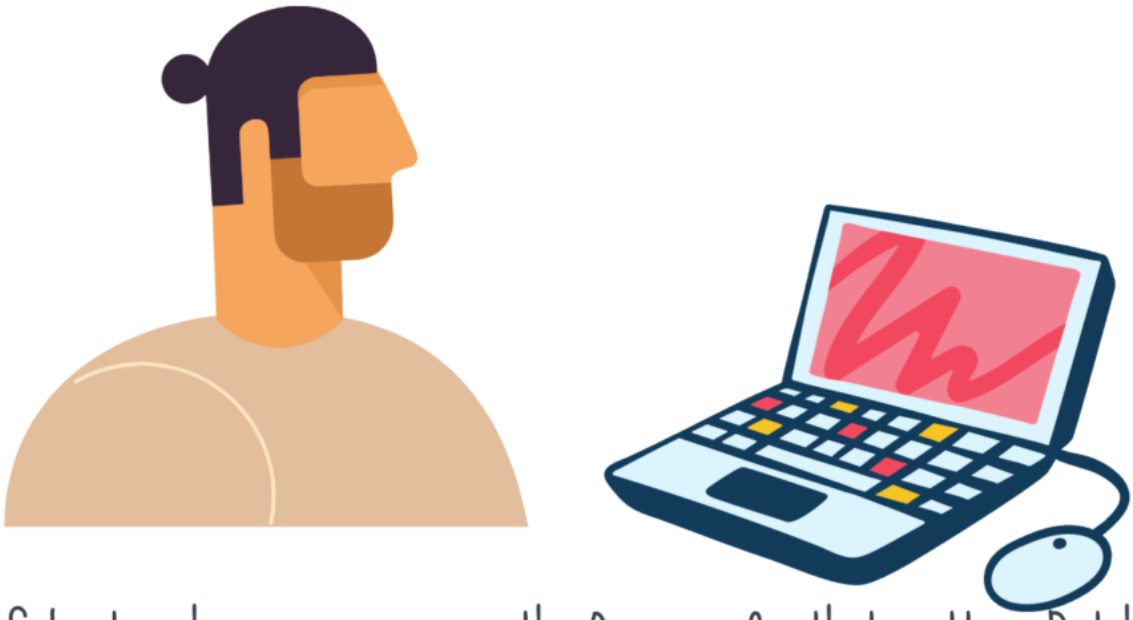
OPSGROUP Team
24 June, 2021

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.



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.

Subject: A really worthy cause which you should be aware of.

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [redacted] only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
[redacted]

http://ww[redacted]

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 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.

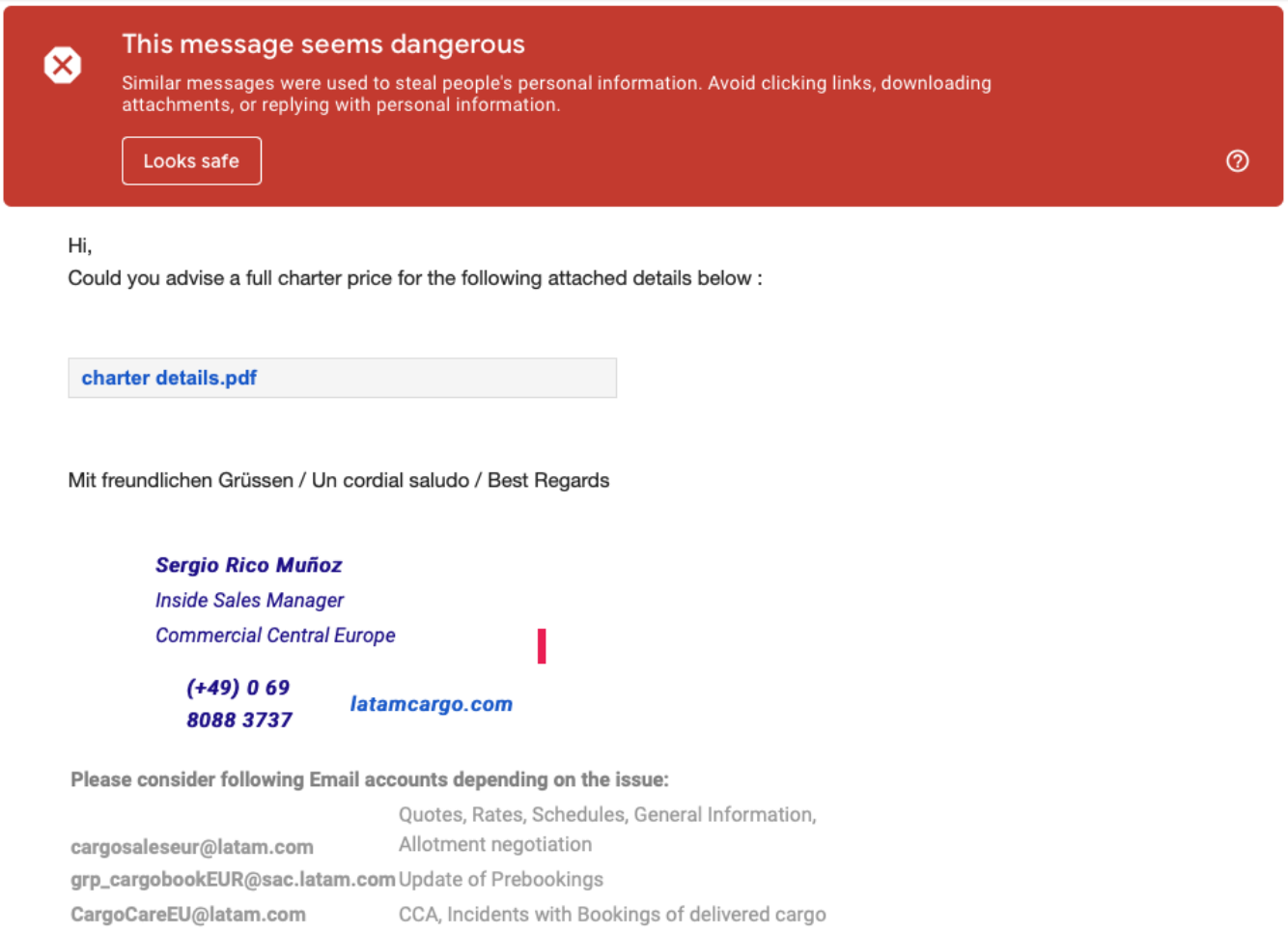
What are we seeing at OPSGROUP?

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.



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.

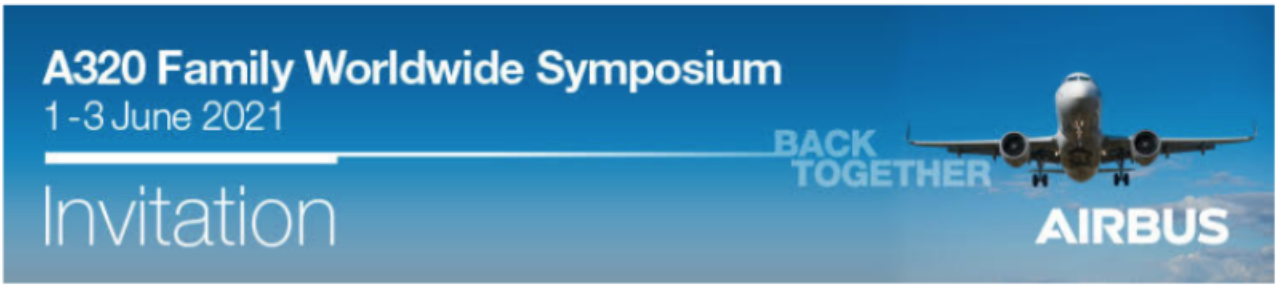
Microsoft put a warning out earlier in 2021 saying they are tracking this 'dynamic' campaign which is targeting the aerospace and travel sectors with **spear-phishing emails**. When the PDF in the email is opened it delivers RevengeRAT or AsyncRAT to your computer.

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> Thu, Apr 29, 2021 at 11:46 AM
Reply-To: non-reply@airbus.com



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 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.