

Russian CAA website taken offline

OPSGROUP Team

29 March, 2022



On March 29, the entire Russian Civil Aviation Authority website went offline. Hackers are saying they managed it, Russian media is saying it is down to restructuring.

Either way the website currently isn't available, so if you need to get in touch it will have to be via good old fashioned postal service or AFTN.

What's offline?

www.favt.ru currently isn't responding. This is the **'Rosaviatsia' Federal Agency for Air Transport** site which manages civil aviation across Russia.

www.scaa.ru also doesn't respond.

AvHerald reported that the site has been hacked, and all backup data also erased.

What does this mean?

With few external operators flying in and out of Russia it might not mean much right now. However, if you are trying to fly in or contact them then this may pose issues for you until they get their site back up and running.

Things like **permissions and permits** will undoubtedly take longer to get hold of.

Whether there will be any further indirect impact on other aviation related service within Russia is not yet clear.

The Contact Info.

Contact via post of AFTN are your best bets, but you can try calling as well. It isn't clear if email will be available.

Telephone: +7 499 231 5237

Email: aviapermit.scaa.ru / rusavia@scaa.ru / permit@matfmc.ru

AFTN: UUUUYAYX / UUUUKZXTD

SITA: MOWYAYA / MOWICYA

Address: 125993, GSP-47, Moscow, Leningrad Prospekt, 37, building 2

Any local agent contacts?

Aerotrans may be able to assist: +7 495 755 9422 / handling@CPDU.ru

Alternatively you may do best to contact local agents at your airport of operation directly as it may be easier for them to coordinate for you.

Please be Wary of Malicious Phish

OPSGROUP Team

29 March, 2022



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 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.

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.

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.

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.

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.

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.