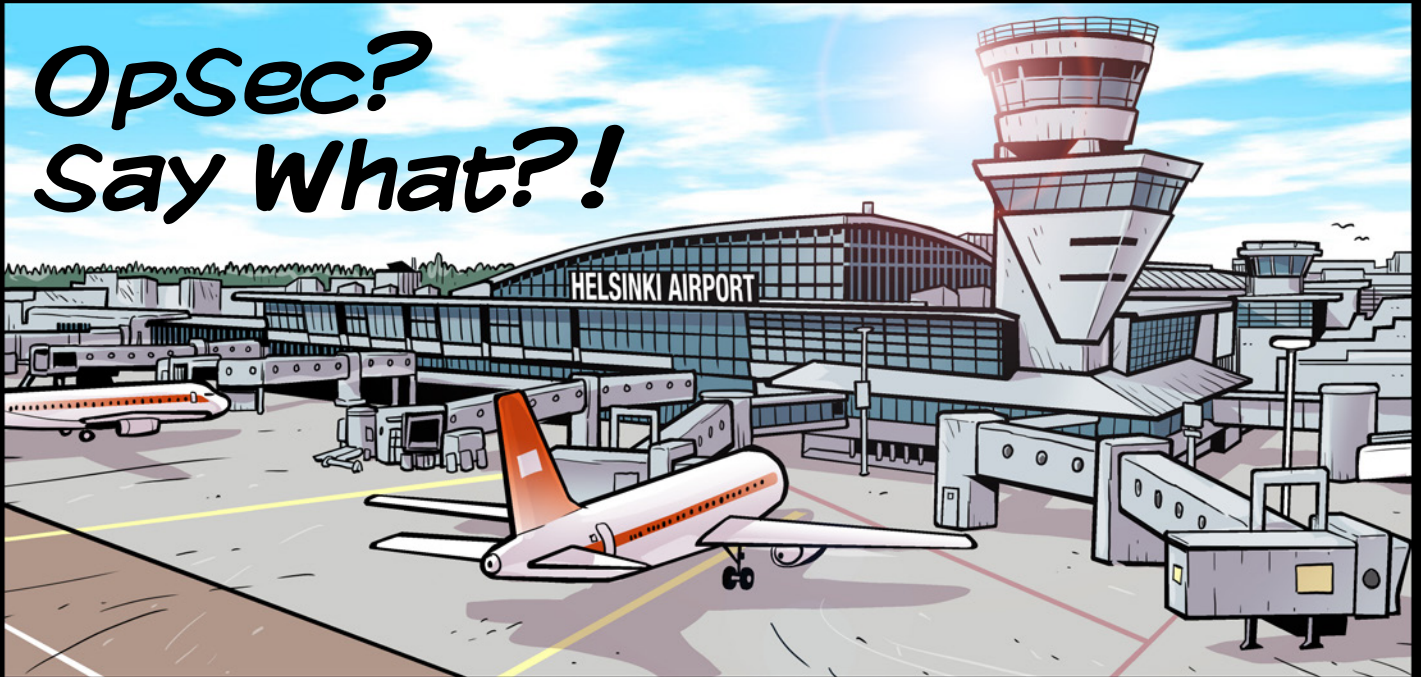
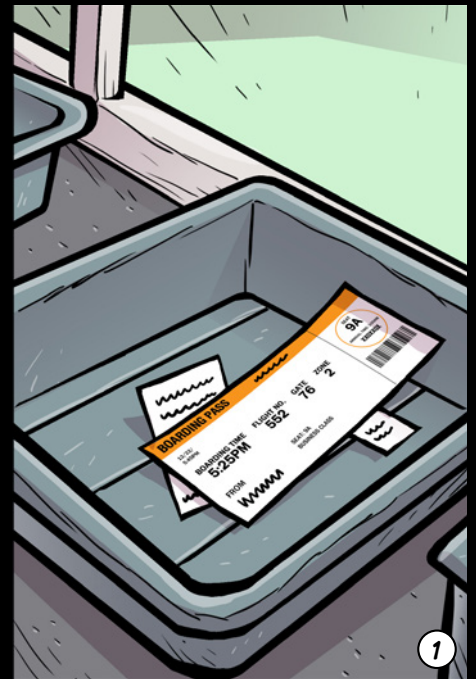


OpSec? Say What?!



YET ANOTHER BUSINESS TRIP



MINUTES BEFORE THE FLIGHT

Let's find a charging
station.



I'll quickly send
the latest data to
Matthew.





PREPARING FOR THE MEETING



THE NEXT MORNING

Acme Corporation

Good morning!
Shall we get started?

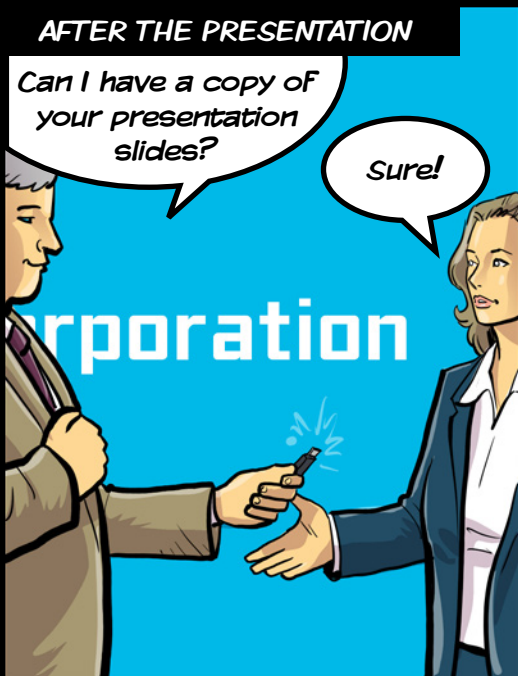
Yes, please
do.



AFTER THE PRESENTATION

Can I have a copy of
your presentation
slides?

Sure!



Thanks For
Flying over.

Thanks. You'll
hear from us
soon.



IN THREE WEEKS...



10 TIPS FOR BUSINESS OPSEC



- 1 Take good care of your belongings. All it takes for a stranger to get access to your full travel plan is a quick look at the last name and booking reference on your boarding pass.
- 2 Plug your devices only to trusted ports. If a port is compromised, there's no limit to what information could be taken from your device, or what gets installed on it.
- 3 Always use VPN for protecting your network traffic. Favor instant messaging such as Signal Private Messaging for sending sensitive information.
- 4 Carefully choose the locations where you share confidential information. A person with noise-cancelling headphones can hear your discussion despite the noise on the plane.
- 5 Carry your devices with you whenever possible. Avoid using hotel safes.
- 6 Take all valuable items and work-related documents with you, instead of leaving them lying around.
- 7 Make active decisions on what you share, with whom, and where. Even mundane information can be useful for someone.
- 8 Store passwords in a password manager. Use generated passwords, and memorize the most important ones. Never reuse passwords.
- 9 Always run the latest version of your operating system, and turn on auto updates. Favor iOS devices or Chromebooks, and use Chrome as your browser.
- 10 Never plug unknown peripherals into your devices. Not even if they are from a person you know well.

Maintaining good OpSec for long periods of time can be stressful. You have to repeat some things over and over. And then there are things you need to be careful not to repeat too often. It's not easy. But remember: when it comes to OpSec, doing something is always better than doing nothing.