CROSSING THE BORDER

Presented by:

Karl Larson
October 28, 2019

About me

- TELUS Security Director & Chief Information Security Officer
- 20+ years' experience in Information Security and Information Technology in Canada, the United States and Europe

Agenda

- Travel security in the news
- Preparing for your trip
- In transit and out of country

Sounds paranoid?

> *"The transportation industry became the second-most attacked sector in 2018 – moving up the ranks from 10th in 2017."*

IBM X-Force Threat Intelligence Index
February 2019

Since January 2018, more than 566 million travel industry records have been leaked

Travel security is in the news

Business

Canada Border Services seizes lawyer's phone, laptop for not sharing passwords

Concern is mounting over Canadian border officers' powers to search smartphones

Sophia Harris · CBC News · Posted: May 05, 2019 4:00 AM ET | Last Updated: May 5

A Canadian border officer seized lawyer Nick Wright's laptop and phone when he wouldn't hand over his passwords. (submitted by Nick Wright)

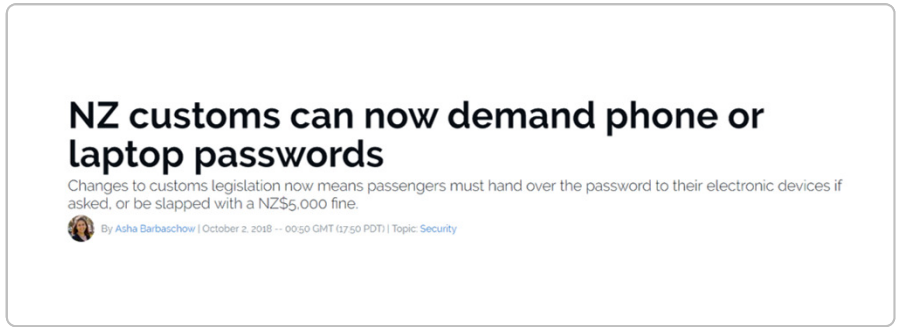
Technology

Apple employee detained by U.S. customs agents after declining to unlock phone, laptop

Customs and Border Protection officers violated a citizen's rights when they demanded he turn over passwords to his electronic devices at the airport, the American Civil Liberties Union Foundation of Northern California said in a civil complaint filed Tuesday. (Daniel Acker/Bloomberg)

By **Hamza Shaban**
April 3

Reports highlight civil rights and privacy issues …



NZ customs can now demand phone or laptop passwords

Changes to customs legislation now means passengers must hand over the password to their electronic devices if asked, or be slapped with a NZ$5,000 fine.

By Asha Barbaschow | October 2, 2018 -- 00:50 GMT (17:50 PDT) | Topic: Security

STEP THIS WAY, PLEASE —

Woman: My iPhone was seized at border, then imaged—feds must now delete data

Lawyer: "They provided no justification for why they took the phone."

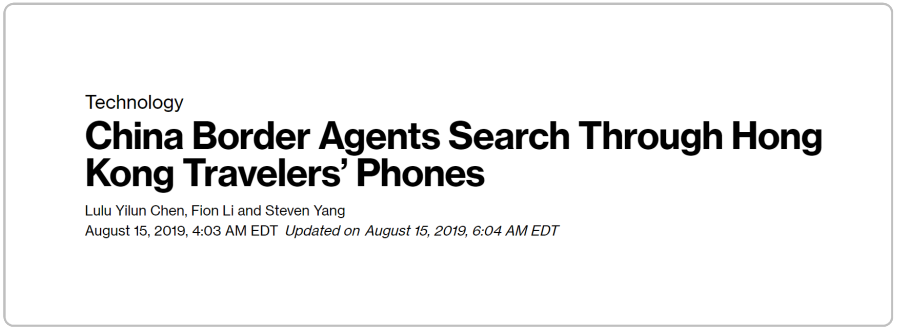
CYRUS FARIVAR - 8/23/2018, 10:00 AM

MOBILE

China reportedly scans tourists' phones by installing malware

The app, which downloads texts, call logs and calendar entries, is installed when tourists cross certain borders, according to an investigative report.

BY CORINNE REICHERT | JULY 2, 2019 11:54 AM PDT



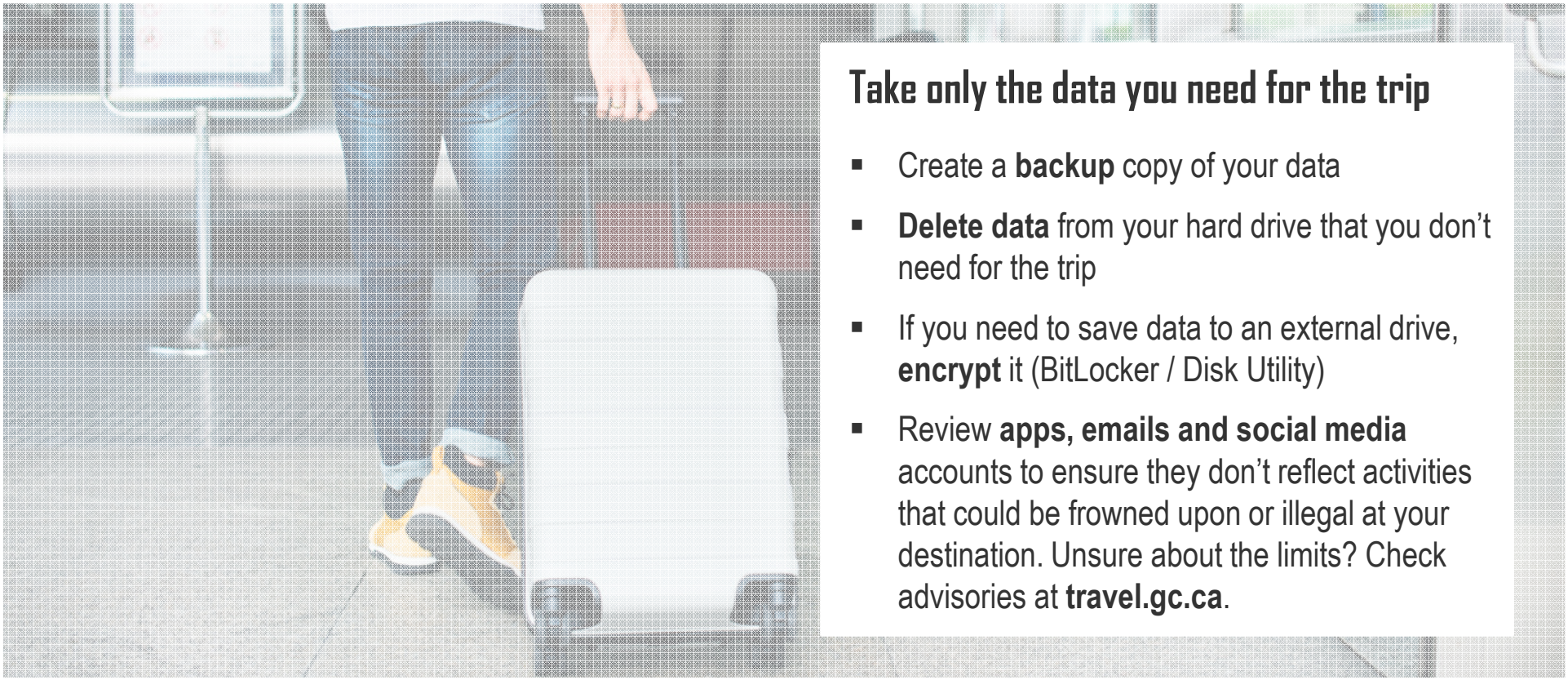
Technology

China Border Agents Search Through Hong Kong Travelers' Phones

Lulu Yilun Chen, Fion Li and Steven Yang
August 15, 2019, 4:03 AM EDT *Updated on August 15, 2019, 6:04 AM EDT*

… but the underlying issue is how much sensitive information we carry

Travel security hinges on good data management



Take only the data you need for the trip

- Create a **backup** copy of your data
- **Delete data** from your hard drive that you don't need for the trip
- If you need to save data to an external drive, **encrypt** it (BitLocker / Disk Utility)
- Review **apps, emails and social media** accounts to ensure they don't reflect activities that could be frowned upon or illegal at your destination. Unsure about the limits? Check advisories at **travel.gc.ca**.

Think about the devices you need to take with you

Laptop

If you think you're going to use public Wi-Fi, consider signing up for a VPN

Smartphone

Log off as many apps as you can before you leave and consider deleting ones you don't need

Charger

Public charging stations & borrowed cables can be altered to allow access to your device – bring a cable that **plugs into voltage**

"Live life with no excuses, travel with no regret."

– Oscar Wilde

If you're travelling with work devices, check your organization's security policy

At the airport: dealing with customs

If an officer asks to see your device:

- Put it in airplane mode, key in the password and **hand it over**
- Make sure you **know what data** is on your device, so you can answer questions easily
- **Log off accounts** before you hit customs so that agents need to ask you for multiple passwords to see everything

Given that you are consenting to the search, this is not considered a privacy breach.

In the airport lounge and on the plane

Avoid public Wi-Fi

If public Wi-Fi is unavoidable:

- Be cautious about the data you share
- Use a VPN

Switch Bluetooth off

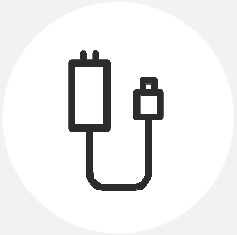
If your Bluetooth is on, your device will sync up automatically with nearby devices and networks

Keep devices on you

Always have your devices on your person and only store them in carry-on luggage

Watch for shoulder surfers

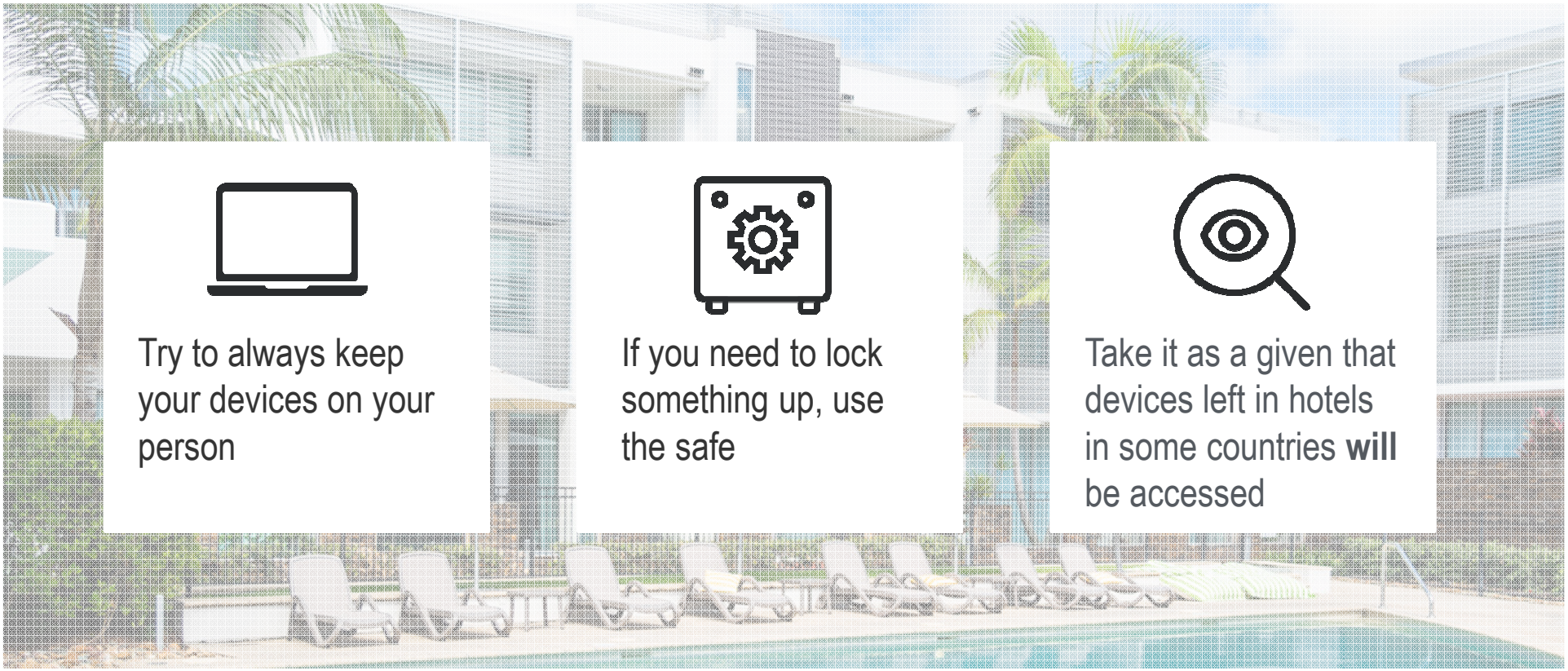
Ensure nobody is reading your screen and be mindful about having business conversations in public



Avoid public charging stations

Take your own power bank or a cable that can plug in to voltage

At the hotel



Try to always keep your devices on your person

If you need to lock something up, use the safe

Take it as a given that devices left in hotels in some countries **will** be accessed

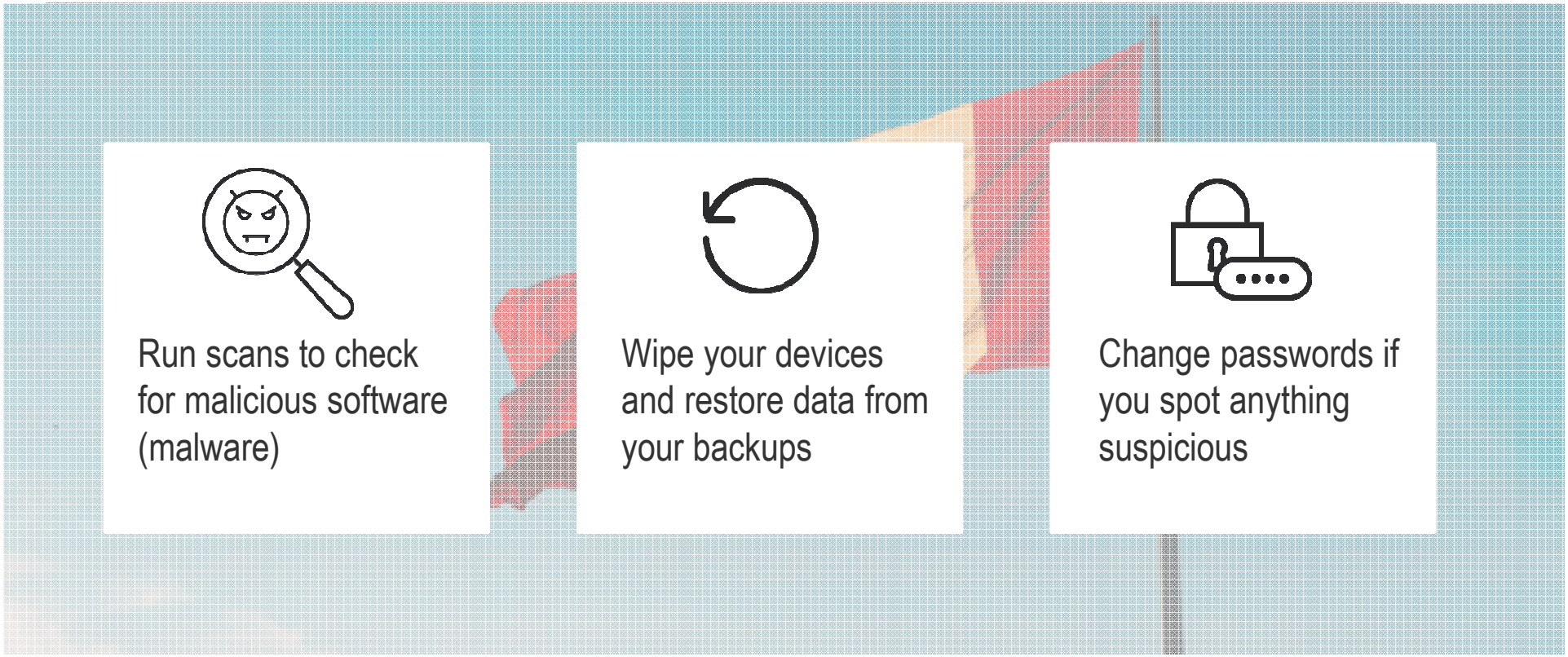
When you’re out and about

Steer clear of public computers – they are a significant risk

Avoid public Wi-Fi and switch off Bluetooth

Try to keep your devices on your person at all times

When you arrive home



Run scans to check for malicious software (malware)

Wipe your devices and restore data from your backups

Change passwords if you spot anything suspicious

Know what to do if your device gets stolen

- Enrol in a “find my device” option before you leave
- Take your service provider’s contact information with you
- Report theft to local police

Resources

- **Queen's ITS security awareness**
  queensu.ca/its/security
- **Queen's Traveling Abroad Tip Sheet**

QUESTIONS?