# Malicious actors trying to exploit global tech outage for their own gain

July 21 2024, by DAVID KOENIG and JILL LAWLESS


An IT field services technician works on software on an information display near United Airlines gates at Chicago O'Hare International Airport, in Chicago, Friday, July 19, 2024. Transport providers, businesses and governments are rushing to get all their systems back online after long disruptions following a widespread technology outage. Credit: AP Photo/Carolyn Kaster

As the world continues to recover from massive business and travel disruptions caused by a faulty software update from cybersecurity firm CrowdStrike, malicious actors are trying to exploit the situation for their own gain.

Government cybersecurity agencies across the globe and CrowdStrike CEO George Kurtz are warning businesses and individuals about new phishing schemes that involve malicious actors posing as CrowdStrike employees or other tech specialists offering to assist those recovering from the outage.

"We know that adversaries and bad actors will try to exploit events like this," Kurtz said in a statement. "I encourage everyone to remain vigilant and ensure that you're engaging with official CrowdStrike representatives."

The UK Cyber Security Center said they have noticed an increase in phishing attempts around this event.

Microsoft said 8.5 million devices running its Windows operating system were affected by the faulty cybersecurity update Friday that led to worldwide disruptions. That's less than 1% of all Windows-based machines, Microsoft cybersecurity executive David Weston said in a blog post on Saturday.

He also said such a significant disturbance is rare but "demonstrates the interconnected nature of our broad ecosystem."

## What's happening with air travel?

With their tightly timed, interwoven schedules and complex technology systems, many big airlines struggle to stay on time when everything goes well. It perhaps was not surprising that the industry was among the

hardest hit by the outage, with crews and planes caught out of position.

By mid-afternoon Saturday on the U.S. East Coast, airlines around the world had canceled more than 2,000 flights, according to tracking service FlightAware. That was down from 5,100-plus cancellations on Friday.

About 1,600 of Saturday's canceled flights occurred in the United States, where carriers scrambled to get planes and crews back into position after massive disruptions the day before. According to travel data provider Cirium, U.S. carriers canceled about 3.5% of their scheduled flights for Saturday. Only Australia was hit harder.

Canceled flights were running at about 1% in the United Kingdom, France and Brazil and about 2% in Canada, Italy and India among major air-travel markets.

Robert Mann, a former airline executive and now a consultant in the New York area, said it was unclear exactly why U.S. airlines were suffering disproportionate cancellations, but possible causes include a greater degree of outsourcing of technology and more exposure to Microsoft operating systems that received the faulty upgrade from CrowdStrike.


Jose Angel Saavedra, left, and his wife Sara, of Johnston, Iowa, look at their cell phones while trying to book a flight after their original flight was cancelled, Friday, July 19, 2024, at the Des Moines International Airport in Des Moines, Iowa. Credit: AP Photo/Charlie Neibergall

## Which airlines are getting hit the hardest?

Delta Air Lines canceled more than 800 flights, or one-fourth of its schedule for Saturday, and that number did not include Delta Connection regional flights. It was followed by United Airlines, which dropped nearly 400 flights.

The worst airport to be, for a second straight day, was Hartsfield–Jackson Atlanta International Airport, where Delta is the

dominant carrier. The Atlanta Journal-Constitution reported that thousands of people spent the night at the airport, many sleeping on the floors.

European airlines and airports appeared to be recovering slowly, although Lufthansa and its affiliates canceled dozens of flights. Its Eurowings budget subsidiary said check-in, boarding, booking and rebooking flights were all available again, although "isolated disruptions" were possible.

London's Heathrow Airport said it was busy but operating normally on Saturday and that "all systems are back up and running." Flights at Berlin's main airport were departing on or close to schedule, German Press Agency dpa reported, citing an airport spokesman.

## How are healthcare systems holding up?

Health care systems affected by the outage faced clinic closures, canceled surgeries and appointments and restricted access to patient records.

Cedars-Sinai Medical Center in Los Angeles, Calif., said "steady progress has been made" to bring its servers back online and thanked its patients for being flexible during the crisis.

"Our teams will be working actively through the weekend as we continue to resolve remaining issues in preparation for the start of the work week," the hospital wrote in a statement.

In Austria, a leading organization of doctors said the outage exposed the vulnerability of relying on digital systems. Harald Mayer, vice president of the Austrian Chamber of Doctors, said the outage showed that hospitals need analog backups to protect patient care.

The organization also called on governments to impose high standards in patient data protection and security, and on health providers to train staff and put systems in place to manage crises.

"Happily, where there were problems, these were kept small and short-lived and many areas of care were unaffected" in Austria, Mayer said.

The Schleswig-Holstein University Hospital in northern Germany, which canceled all elective procedures Friday, said Saturday that systems were gradually being restored and that elective surgery could resume by Monday.


Passengers wait at Benito Juárez International Airport in Mexico City, Friday, July 19, 2024. Some flights were canceled and others were delayed amid a global technology outage. Credit: AP Photo/Marco Ugarte

## Will the tech industry face a reckoning?

"I wasn't that surprised that an accident caused severe global digital disruption. I was a little surprised that the cause of it was a software update from a very well-respected cybersecurity company," said Oxford University management professor Ciaran Martin, a former chief executive of the U.K.'s National Cyber Security Center.

"There are some very hard questions for CrowdStrike. How on earth did this update get through quality control?" he said. "Clearly the testing regime, whatever it is, failed."

Martin said governments in the U.K. and the European Union will be powerless to take steps to prevent such breakdowns "because we have become dependent on a very American version of technology, and the power to do anything about that doesn't rest in this continent."

Other analysts doubted that the outage would lead Washington or any other government to propose new mandates on tech companies.

"I don't know what the mandate would be. Do better QA?" said Gartner analyst Eric Grenier, using an acronym for quality assurance.

## What did scam artists learn from the outage?

Grenier expects that a majority of affected machines will be fixed in about a week, with more time needed to reach laptops used by far-flung workers because the work can't be done remotely—it's a hands-on operation.

In the meantime, there will be scammers trying to take advantage of

businesses that have indicated they were affected by the outage.

"The threat is very real," Grenier said. "Bad actors have the information to send targeted phishing emails and calls. They know what endpoint-protection tools you use. They know you use CrowdStrike."

Grenier said affected businesses need to make sure they use a fix supplied by CrowdStrike. "Don't accept the help of somebody coming out of the blue and saying, 'I'll fix that for you,'" he said.