

# Hackers publish contact info of 20,000 FBI employees

By Mary Kay Mallonee, CNN

Updated 8:34 PM ET, Mon February 8, 2016



Hackers 'stole a master key' to U.S. government 02:17

## Story highlights

Hackers published contact information for 20,000 FBI employees Monday afternoon

The Justice Department is actively investigating the incident

**Washington (CNN)** — Hackers, making good on their threat, published contact information for 20,000 employees Monday afternoon, just one day after releasing similar data on almost 10,000 Department of Justice employees.

The hackers, tweeting from the account @DcHackers, claim they obtained the details by hacking into the Department of Justice database.

CNN

February 2016

CNET

January 2018

# Homeland Security breach exposes data on 240,000 employees

Personally identifiable information was discovered in the possession of a former department employee.

BY STEVEN MUSIL / JANUARY 3, 2018 6:20 PM PST




8/29/2016  
07:30 AM

---



Alex Campbell  
Commentary

---

 0 COMMENTS  
[COMMENT NOW](#)

---

# Critical Infrastructure: The Next Cyber-Attack Target

**Power and utilities companies need a risk-centric cybersecurity approach to face coming threats.**

The way we think about cyber attacks changed in December 2015, when Ukraine experienced the first recorded power outage caused by a cyber attack. It didn't last long—between one and six hours, depending on the area—but it showed the government, industry, and the public how these attacks could affect the physical world. It's not just personal information and other sensitive data that's at stake. Critical infrastructure is now under threat.

*Dark Reading*

August 2016