

TOP STORIES



HACKERS

Exciting-Sounding 'Cyber Prison Breaks' Worrying the Feds

BY LAURI APPLE

NOV 5, 2011 6:12 PM

Share

Like

19

12,562

29

Trying to capture a single escaped prisoner usually requires a coordinated effort by law enforcement, tips from the public, and sometimes a superhero or two. So just imagine the chaos that would ensue if *thousands* of inmates were suddenly released from their cells. Logistical nightmare in ALL-CAPS.

The possibility of such a major jailbreak occurring has got government officials worrying, [reports the *Washington Times*](#) (which, mind you, is America's zany [Moonie](#) news source, but also its [best Moonie news source](#), and not always [wrong about everything](#)). The Federal Bureau of Prisons is aware of the growing amount of research on prison security system vulnerabilities and, the paper reports, is "taking it seriously." Good to know.

Meanwhile, prison security has become a hot topic at hackers conferences: At the DefCon conference in August, for example, researchers presented info on a simulated cyber prison break they've devised that [shows](#) how security flaws could be easily exploited. All it would take is one dumb

prison guard opening up a toxic "I Wanna Be Your Frennd LVOER!!!" email to set all his orange-suited charges free, sounds like:

During a tour of one U.S. prison, the researchers found a guard in the control room checking his email on a computer that communicates with the system operating the doors. If that guard clicked on a malicious link or attachment, he could trigger a prison break, researchers said.

"If the computer had been attacked, we could open up and close the cell doors," said Tiffany Rad, president of ELCnetworks. "Any time you have a security product, the people operating it need to understand why certain operating procedures are in place."

As the *Times* reports, Rad and her dad, former CIA operations officer John J. Strauchs, appeared at last week's **Hacker Halted** convention in Miami to present their simulated cyber attack and discuss the pressing prison security issues of the day. These include fears that hackers can break into the electrical systems and overloading them (which could unlock all the doors), shut down the closed-circuit teevees, shut down intercoms, break into the cash register in the commissary and enabling poor inmates to help themselves to all the overpriced packaged soups and candy bars; and, worst of all, **cybering all of the cyber**.

How do we know that cyber prison attacks aren't just cyber hype? Because one similar attack has already occurred, the *Times* notes. Many U.S. prisons use the same kinds of computer equipment as power plants and other infrastructural institutions. These systems, called "industrial control systems" (ICS), have "increasingly been targeted by hackers" since 2009, says the *Times*, because hackers broke into the ICS used in Iran's nuclear program and this raised their confidence levels to new hackery heights.

An attack on one prison could create enough drama and chaos to keep Crimestoppers busy for several weeks. If hackers planned a multi-prison hacking operation, *tens of thousands of non-violent drug offenders, embezzlers, and check forgers* (and yes, some rapists, robbers, and murderers) would probably tie us down and malign our faces with unsightly facial tattoos.

[[Washington Times](#). Image via AP]

RELATED STORIES

- We Are Legion: The Story of the Hacktivists: Or, 10 Guy Fawkeses
- It Pays to Be the Face of Anonymous
- America: China Is Constantly Hacking Us—China: We're Not GIZMODO