

This content was printed from **Data Center Knowledge**



Legendary hacker Kevin Mitnick on stage at Data Center World 2017 at the Los Angeles Convention Center (Photo: Kyle Espeta for Data Center World)

DATA CENTER WORLD, FEATURED, SECURITY

This Hacker Can Talk His Way inside a Data Center

When a credit bureau hired Kevin Mitnick's company to test its security defenses, he went straight for the crown jewels. He decided he would try to get inside the bureau's data center, physically, on his own two feet.

After spending the second half of the nineties in prison for a number of computer crimes, he did not quit hacking. Instead, the legendary former cybercriminal put together an entire team of hackers who break into organizations' systems using his signature combination of in-person deceit (Mitnick is a top authority on social engineering) and technological exploits as a service, to help them identify security holes.

This week, on stage at the Los Angeles Convention Center during the annual [Data Center World](#) conference, Mitnick demonstrated in real-time an entire list of ways one could get proprietary and personal information, using both internet search skills and sophisticated technological exploits, from personal computers as well as corporate networks.

One of the tools he's used is a device that reads identification code from access badges by HID, common in corporate offices and data centers. Once it reads the code, the badge can be easily cloned, giving the hacker the same physical access as the badge's owner.

Mitnick had to clone two badges to get inside this particular client's data center: one to get into the building and the other to get inside the data hall. He used social engineering (the art of manipulating people into disclosing valuable information) to get his hands on the first one.

Since the data center was inside an office building operated by a real estate company, he called and set up an appointment with a salesperson, pretending to be interested in leasing office space. During the tour, he casually asked how the company managed access control, and the salesperson showed him her badge. He asked to take a closer look, and she handed the badge to him, at which point he held it next to a leather planner he was holding, with the badge reading device inside. He only needed to hold the badge for a second to clone it.

Once the device reads the target's badge, all it takes is holding a blank badge over it to transfer the code.

To get to a badge that would get him inside the actual bureau data center, Mitnick needed to clone one that belonged to a person that worked in the facility. He could already freely walk around the building, so he went into a men's restroom that was closest to the data center and waited until he could stand at a stall next to one of the data center's employees, at which point all he needed was to briefly get his planner close to the badge hanging on the target's belt.

Of course, access badges are eventually going to give way to more advanced access-control technologies, such as biometric identification and facial recognition, but it will be a while before all legacy enterprise data centers will upgrade their physical security systems with the latest and greatest fingerprint and iris scanners and machine-learning technology that will recog-

nize whether a person in a CCTV video is supposed to be on the data center floor.

While finding a technological exploit to break into a system is just a matter of time for sophisticated hackers, people are still the weakest link in any cybersecurity scheme today, Mitnick said. "Human factor — that's usually the easiest way in."

Attacks that exploit that human factor – like the March 2016 [spear-phishing email](#) to former chairman of Hilary Clinton's presidential campaign John Podesta that eventually put sensitive campaign emails into the hands of WikiLeaks – are a favorite type of exploit by cybercriminals.


"These attacks are very common and usually the easiest way in," Mitnick said.


Get Daily Email News from DCK!
Subscribe now and get our special report, "The World's Most Unique Data Centers."
Email* **Country***

SUBSCRIBE

Enter your email to receive messages about offerings by Penton, its brands, affiliates and/or third-party partners, consistent with Penton's [Privacy Policy](#).

About the Author



Yevgeniy Sverdlik (1380 Posts) 

San Francisco-based business and technology journalist. Editor in chief at Data Center Knowledge, covering the global data center industry.

Inside DCK	Hot Topics	News Channels	Stay Connected
About Us	DCIM News	White Papers	Daily Email Newsletter
Advertise	Downtime	Events Calendar	RSS
Staff	HPC / Supercomputing	Virtualization	Twitter
Contact Us	Facebook	Consolidation	Facebook
Submit News	Apple	Open Compute	LinkedIn
Submit Guest Column	Microsoft	Internet of Things	Data Center Videos
Site Map	Google	Storage	Humor
	Northern Virginia	Convergence	Webinars
	New York	Disaster Recovery	
	Silicon Valley	Managed Hosting	
	North Carolina	Content Delivery	
		Site Selection	
		Investing	

Visit our other properties:

Hosting and Cloud Web Hosting Talk, HostingCon, WHIR, Hosting Catalog, Hottest Hosts

Data Center Data Center Knowledge, Data Center World, AFCOM

Web Development Hot Scripts, DB Forums **Performance Marketing** ABestWeb

Consumer Tech Windows Secrets, Overclockers, Mac Forums

Penton Privacy Policy, Terms of Services, Advertise

Hosting By:
Powered by 