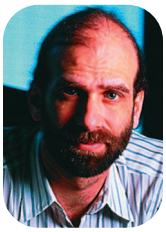
Airplane Hackers

Nathaniel Heatwole is a student at Guilford College. Several times between 7 February and 15 September 2003, he tested airline security. First, he smuggled in box cutters, clay resembling plastic explosives, and bleach simulating bomb-making chemicals through security. Then he hid these things in airplane lavatories, along with notes. Finally, he sent an email to the US Transportation Security Administration (TSA) titled "Information Regarding Six Recent Security Breaches."



Bruce Schneier
Counterpane Internet Security

The problem is that the TSA never asked him to test its security. In this same vein, computer networks have been plagued for years by hackers breaking into them. But these people aren't breaking into systems for profit; they don't commit fraud or theft. They're breaking into systems to satisfy their intellectual curiosity, for the thrill, and just to see if they can.

Hackers' traditional and common defense is that they're breaking into systems to test their security. They say the only way to learn about computer and network security is to attack systems. Never mind that these hackers don't own the systems they're breaking into; that's just the excuse.

The US Department of Homeland Security and the TSA have been attacked by their first hacker. He wasn't a terrorist; he wasn't out to take over the planes. He isn't even a criminal; he didn't try to extort money. He was a hacker, plain and simple. He wanted to test the security screeners' efficacy, to demonstrate that our airport security measures are, in his eyes, inadequate. He wanted to hack airport security.

Heatwole's whole escapade is extraordinarily silly. Every traveler I know has stories of knives that airport security missed. No one who regularly flies thinks the TSA is doing a good job of keeping sharp objects off airplanes. Even worse, no one who regularly flies thinks that keeping sharp objects off airplanes makes us all safer. Most of what the TSA does is security theater—window dressing. It keeps up appearances, and maybe (hopefully) makes terrorists less sure they can smuggle weapons aboard airplanes. Probably not.

Heatwole's actions are, and should be treated as, a crime. "I was only testing security" is not a valid defense. For years, we in the computer-security field have heard that excuse. Because the hacker didn't intend harm, because he just broke into the system and merely looked around, it wasn't a real crime. Here's a thought for you—imagine you return home and find the following note attached to your refrigerator: "I was testing the security of back doors in the neighborhood and found yours unlocked. I just looked around. I didn't take anything. You should fix your lock." Would you feel violated? Of course you would.

That said, although Heatwole's actions were criminal, they weren't terribly serious. His stunt was embarrassing, and cost a whole lot of money to investigate and clean up. It could have disrupted lots of people's travel schedules. But he's not a terrorist. He didn't do this to feed security information to al-Qaida. His actions didn't endanger anyone's lives. There's a tendency to want to throw the book at him because he embarrassed important government officials, but that's not a good enough reason. We need to discourage this behavior, but the punishment needs to fit the crime. Treat Heatwole as a criminal, but not a serious criminal.

Welcome to our world, Department of Homeland Security. Welcome, TSA. We've been fighting these sorts of people for years. You're going to have better luck prosecuting them, but don't let your anger get in the way of reason. □

***Bruce Schneier** is one of the world's foremost security experts and Counterpane Internet Security's chief technology officer. His new book,* Beyond Fear: Thinking Sensibly about Security in an Uncertain World, *was published in September. Contact him at www.schneier.com.*

Ed. Note: A version of this column appears in Bruce Schneier's Crypto-Gram *newsletter (www.schneier.com/crypto-gram.html).*