

March 18, 1998

U.S. Department of Justice

**Press Contact: Amy Rindskopf
(617) 223-9445
Boston, MA**



Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport

First Federal Charges Brought Against a Juvenile for Computer Crime

BOSTON, MA ... Federal criminal charges were unsealed today against a computer hacker who disabled a key telephone company computer servicing the Worcester airport. As a result of a series of commands sent from the hacker's personal computer, vital services to the FAA control tower were disabled for six hours in March of 1997. In the course of his hacking, the defendant also electronically broke into a pharmacy computer and copied patient records. The charges announced today by United States Attorney Donald K. Stern and Acting Special Agent in Charge Michael T. Johnston of the U.S. Secret Service are the first ever to have been brought against a juvenile by the federal government for commission of a computer crime. In accordance with federal law, the juvenile was not publicly named.

U.S. Attorney Stern stated: "Computer and telephone networks are at the heart of vital services provided by the government and private industry, and our critical infrastructure. They are not toys for the entertainment of teenagers. Hacking a computer or telephone network can create a tremendous risk to the public and we will prosecute juvenile hackers in appropriate cases, such as this one."

The criminal charges contained in the Information allege that the computer hacker temporarily disabled Next Generation Digital Loop Carrier systems ("loop carrier systems") operated by NYNEX (later purchased by Bell Atlantic Telephone Company) at the Worcester Airport and in the community of Rutland, Massachusetts. Loop carrier systems are programmable remote computers used to integrate voice and data communications originating on a large number of standard, copper-wire telephone lines for efficient transmission over a single, sophisticated fiber-optic cable.

In many respects, a loop carrier system serves the same function as a circuit breaker box in a home or an apartment. Individual electric wires do not run from each plug or light in a home or apartment to the electric company. Rather, the myriad of plugs and lights are connected to a circuit breaker box in a corner of the home or apartment, to which the electric company attaches a single, efficient cable. If the circuit breaker box is disabled, however, none of the lights and outlets in the house can function. Loop carrier systems are used by telephone companies to integrate service provided over hundreds of telephone lines for digital transmission over a single, high capacity fiber-optic cable to a central office.

"Just as disabling a circuit breaker box blacks out an entire house, so disabling a loop carrier system cuts off all communications with the telephone lines it services," explained U.S. Attorney Stern.

The Information alleges that the loop carrier systems operated by the telephone company were accessible from a personal computer's modem. This accessibility was maintained so that telephone company technicians could change and repair the service provided to customers by these loop carrier systems quickly and efficiently from remote computers.

The juvenile computer hacker identified the telephone numbers of the modems connected to the loop carrier systems operated by the telephone company providing service to the Worcester Airport and the community of Rutland, Massachusetts. On March 10, 1997 he accessed and disabled both in

sequence.

Acting Special Agent in Charge Johnston stated, "This case, with the associated national security ramifications, is one of the most significant computer fraud investigations conducted by the U.S. Secret Service."

At approximately 9:00 a.m., the juvenile computer hacker intentionally, and without authorization, accessed the loop carrier system servicing the Worcester Airport. He then sent a series of computer commands to it that altered and impaired the integrity of data on which the system relied, thereby disabling it. Public health and safety were threatened by the outage which resulted in the loss of telephone service, until approximately 3:30 p.m., to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to other related concerns such as airport security, the weather service, and various private airfreight companies. Further, as a result of the outage, both the main radio transmitter, which is connected to the tower by the loop carrier system, and a circuit which enables aircraft to send an electric signal to activate the runway lights on approach were not operational for this same period of time.

Later on the same day, at approximately 3:30 p.m., the juvenile computer hacker intentionally, and without authorization, accessed the loop carrier system servicing customers in and around Rutland, Massachusetts. Once again, he sent a series of computer commands to the digital loop carrier that altered and impaired the integrity of data on which the system relied, thereby disabling it. The second outage disrupted telephone service throughout the Rutland area, causing financial damage as well as threatening public health and safety as a result of the loss of telephone service. During this attack, the juvenile computer hacker changed the system identification to "Jester".

U.S. Attorney Stern commended Bell Atlantic, which brought the situation to the attention of the Secret Service and his office after it determined that the security of its network had been breached. Stern said: "Technology is never going to create perfect security. As a result of Bell Atlantic's quick reaction and invaluable assistance, the Secret Service was able to identify a vulnerability that affected not only the two telephone company computers hacked in this case, but hundreds of identical computers used by Bell Atlantic around New England and thousands used by telephone companies around the country. Our critical infrastructure is safer because of Bell Atlantic's intolerance of the intrusions it discovered into its network."

Acting Special Agent in Charge Johnston added, "The success of this investigation, as well as previous and other on-going investigations, demonstrates the cooperation that has developed between law enforcement agencies and private industry in the suppression of electronic crimes. The U.S. Secret Service would like to recognize the invaluable assistance provided by the Bell Atlantic Corporation."

The Information also alleges that, in a separate computer intrusion, the juvenile computer hacker used his personal computer and modem to break into the pharmacist's computer in a Worcester area branch of a major pharmacy chain. The pharmacist's computer was accessible by modem after hours when the pharmacy was closed. This accessibility was maintained so that the pharmacy chain could periodically transfer information from the pharmacist's local computer to a centralized computer operated by the chain in the course of its business.

The juvenile computer hacker identified the telephone number associated with the modem servicing the pharmacist's computer in the Worcester pharmacy. On four occasions in January, February and March of 1997, the juvenile computer hacker used his personal computer modem to break into the Worcester pharmacy computer. On each of these days he instructed the Worcester pharmacy computer to transmit to his personal computer files containing all of the prescriptions filled by the pharmacy during the previous week, detailing them by customer name, address, telephone number and prescription medicine supplied.

"While he could not alter the prescriptions and we found no evidence that he disseminated the information, this constituted a serious invasion of privacy," said Stern.

Pursuant to a plea agreement, the juvenile will receive two years' probation, during which he may not possess or use a modem or other means of remotely accessing a computer or computer network directly or indirectly, must pay restitution to the telephone company and complete 250 hours of

community service. In addition, he has been required to forfeit all of the computer equipment used during his criminal activity.

Addressing the decisions to prosecute and reach a plea agreement, Stern stated: "This case reflects our intention to prosecute in federal court anyone, including a teenager, who commits a serious computer crime. The plea agreement is a balanced effort, weighing the seriousness of this juvenile's computer intrusions and his lack of malevolence. As with a driver's license, the freedom to explore with a computer and modem comes with the obligation to act responsibly and respect the law."

The case was investigated by the U.S. Secret Service with the cooperation and assistance of Bell Atlantic Telephone Company and the U.S. Postal Inspection Service, Massachusetts State Police, Office of Inspector General of the Social Security Administration, Oxford Police Department, Leicester Police Department and Rutland Police Department. The U.S. Attorney's Office was assisted by Attorney General Scott Harshbarger's Office and Worcester County District Attorney John J. Conte's Office. It is being prosecuted by Assistant U.S. Attorneys Stephen P. Heymann, Deputy Chief of the Criminal Division of the U.S. Attorney's Office and Allison D. Burroughs, of Stern's Economic Crimes Unit.

Press Contact: Amy Rindskopf, (617) 223-9445

###