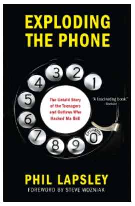

Title **Home Computer as a Weapon For Telecommunications Thief**

Publication *The Washington Post*

Date 1978-06-23

Author(s) Schrage, Michael

V/I/P p. B13

Abstract Captain Crunch pleads guilty to the first reported case of a crime using a personal computer; he used an Apple II with a telephone interface board to access telephone lines. Article describes early cases of computer crimes, and describes the worry that the growing personal computer market may make computer crime easy and prevalent.

Keywords American Telephone & Telegraph Co. (AT&T); John Draper; Captain Crunch; blue box; computer hackers; personal computer; Donn Parker (sr. mgmt. consultant, SRI International); Senate Bill 1766; Federal Computer Systems Protection Act

Source An anonymous phone phreak

Home Computer as a Weapon For Telecommunications Thief

By Michael Schrage
Special to The Washington Post

NEW YORK—To the folks at American Telephone & Telegraph Co., Captain Crunch is not just a breakfast cereal. Captain Crunch is the nickname of of John Draper, a 35-year-old technical wizard who won notoriety for the skill and ease with which he cracked the Bell System security to place thousands of dollars worth of free calls around the world.

Draper's key to the Bell System was a device known as a "blue box," a multifrequency tone generator that enabled Draper to detect and tap in to Bell customers' WATS lines to make his free phone calls. Luck and months of research were required before the Bell System could track Draper down and amass enough evidence to convict the blue box bandit and send him to prison.

John Draper, alias Captain Crunch, now faces the possiblity of going to prison again. Last Monday, in a Stroudsburg, Pa., courtroom, Draper pleaded guilty to the charge that he was in "possession of a device used, adapted, or manufactured for the commission of a telecommunications theft."

Yet that device was not an ordinary blue box. When authorities arrested John Draper he had in his possession an Apple II personal computer. The computer, which retails nationally for under $1500, was equipped with a telephone interface board that effectvely hooked the computer into the phone lines.

Draper insists that the computer hookup was for legitimate purposes, such as automatic redialing, data transmission, and WATS extending.

Ralph A. Matergia, the prosecuting attorney who spent nearly a year preparing for the case, agrees that there was nothing illegal about the computer/phone interface but points out that the computer was "programmed to probe for phone lines capable of subversion, search for the access codes to those lines, and illegally place calls through those lines."

Matergia asserts that this is a very important case. "This is the first blue box trial concerning the programming abilities of a computer."

It is also the first reported case of a crime involving the use of a personal computer.

The implications of the case are likely to be far broader than the simple conviction of Captain Crunch. The spectre of computer crime has recently haunted business and industry alike. Computer crimes on a national scale cost companies an estimated $100 million annually. And the possibility that computer crimes could be committed by home computer users is a frightening thought to the business community.

Currently, there are an estimated 150,000 home computers around the country. Industry analysts predict that by the end of five years there will be between 1.5 million and 2 million home computers in use. During that time they are expected to become faster, more powerful and more sophisticated. With that increased sophistication comes the increased possibility that the home computer will be used to commit crimes.

"There's no doubt about it. It's a tool and it can be abused," said Van Chandler, the software manager of Radio Shack's TRS-80, a nationally advertised home computer. "However, the level of sophistication for abuse just isn't there yet."

Radio Shack will be coming out shortly with a telephone interface attachment for its home computer and Chandler concedes that, with modification, a TRS-80 with that accessory could be turned into an ultrasophisticated blue box similar to Draper's.

But Donn Parker, a senior management consultant specializing in computer security at SRI International, a non-profit think tank in Palo Alto California, is quick to point out that rapidly evolving improvements of home computer technology make the home computer a threat to nearly all businesses with computers, not just the phone company.

"We're certainly starting to look at it as a potential problem," said Parker. "Personal computer crime presents a significant threat to on-line systems, especially to electronic funds transfer."

Parker postulates that a person with a home computer who can obtain access to a corporate computer system could conceivably subvert and exploit the system for his own benefit.

"The personal computer is more of a threat to such a system than an ordinary computer terminal," Parker said. "The personal computer gives the user a greater amount of leverage."

Rather than place restrictions on home computer technology, Parker calls for developing new and more powerful computer security systems and implementation of data encryption techniques.

Yet the versatility of the home computer is not limited to dealing with other computers. Parker mentions that the home computer could be programmed to simulate or model various situations and events to practice committing a crime.

Moreover, the computer's inherent strengths lend itself to the commission of complex and intricate crimes. Parker relates the story of a London, England, check-kiting scheme of 1975. The game had amassed thousands of pounds illegally be taking advantage of the float between deposits and withdrawals at various banks. The gang had a minicomputer monitor the various transactions to assure that no deposits or withdrawals would be mistimed.

Unfortunately for the criminals, the computer they used malfunctioned, their scheme collapsed, and they were all arrested. While a home computer was not involved in the commission of this crime, Parker asserts that, with proper programming, a home computer could easily have been used.

Of course, computers have had less glamorous partnerships in crime. One computer store owner ruefully tells the story of how she sold a computer to a suspicious looking man who later was arrested for fencing stolen property. His home computer was used to keep track of his inventory.

In an effort to deal with the rising problem of computer crime the Senate Subcommittee on Criminal Law is hearing testimony this week on Senate Bill 1766, the Federal Computer Systems Protection Act.

The act is an omnibus proposal that would outlaw unauthorized use of computers and computer resources. Observers say that the breadth and scope of the bill should discourage those who would commit home computer crimes. It is also felt