CNS /Update Newsletter Feature

Take a Mega-Bite Out of Computer Thefts

CNS Document ID: u960403a
Last Updated: 6/3/99

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
# Table of Contents

- Take a Mega-Bite Out of Computer Thefts .................................................................3
- Rash of Local Computer Crimes ........................................................................3
- Security Measures ............................................................................................3
Take a Mega-Bite Out of Computer Thefts

A dangerous scum is riding the waves of the information revolution. The scum is a growing population of criminals who steal personal computer components, hardware and peripherals. Thefts you've heard about are not isolated incidents. You should worry. The RAM you use to keep a large spreadsheet in memory (while you run a word processor and communicate with colleagues via CNS networks) could be gone tomorrow. The scum can ooze into your unsecured office, envelop your costly CPU motherboard and abscond with it, all in the time it takes you to wander down the hall and back for a cup of coffee. If the scum wants to, it can easily snatch your internal hard drive, and the external backup drive where your life's work is stored -- provided you haven't secured your equipment. At Johns Hopkins University in Maryland, a graduate student lost two years of research data when a hard drive -- along with three high-end Sun CPU systems --were stolen. Hopkins has lost $30,000 in computer equipment in the past few months.

Nationally, this type of crime is growing rapidly, in parallel with the growth of the use of PCs. One of the scum's most frequent victims is educational institutes, from grade schools to universities, because these victims actively promote easy access to computing! Manufacturers have unwittingly helped the scum by making it easy for owners to upgrade their equipment with snap-together cases and "plug-in, pop out" components.

Many CNS customers and their host departments, who increasingly use CNS services from remote microcomputers rather than mainframe terminals, have much to lose. Following are synopses of recent computer crimes in our community, followed by a collection of tips, compiled by Sergeant Nick Vellis of the UF Police Department, on how to thwart computer thieves.

Rash of Local Computer Crimes

According to UF police, 52 cases of computer theft were reported on campus in 1995. Thirty-three full-size desktop computers and five laptops were stolen. The other cases involved theft of computer components, including costly memory and CPU chips, as well as small and large peripherals. UF's self-insurance plan does not cover loss by thefts, so affected departments must figure out individually how (and if) they will be able to replace stolen equipment.

Early this year, a UF student was charged with stealing $4,000 in computer equipment from Fifield Hall. Authorities later estimated that the student had, over time, stolen up to $40,000 worth of equipment. Just weeks ago, UF's student union was a victim, losing a Pentium 133 MHz desktop computer, the CPU and 32MB of RAM from a second machine, and a backup power supply-a $7,000+ loss.

Neighboring Santa Fe Community College was largely spared in 1995. But this year, thieves ransacked a computer lab to the tune of $122,262, all of it in CPU's and memory cards from 100 computers. These components do not generally carry serial numbers and are therefore very difficult to trace and recover.

Security Measures
• Keep all doors and windows in good repair. These items should be checked regularly for adequate security.

• When moving into a new office, have all locks re-keyed.

• Deadbolt locks can be installed on exterior doors (however, note that doors must be "escapable with one hand" to comply with fire code regulations).

• Secure all sliding glass doors or windows, regardless of what floor you are on.

• Lock up even when you are away from your office for just a few minutes.

• Be cautious of strangers in the halls, or people with no apparent destination.

• Use hardware security devices to secure computer equipment to desks or work stations, and to enclose drive cabinets.

• Consider installing a security alarm system. Alarm systems can be effective deterrents, and can be used to notify police in the event of an actual crime. Sometimes simply posting signs on windows and doors indicating an alarm system is present can have a deterring effect.

• Record the equipment's serial number, as well as UF's property record number.

• Engrave university and department names on a conspicuous area of equipment cabinets/enclosures.

• Establish and strictly follow a departmental or office key-control policy.

• Safeguard laptops as carefully as cash.

• Provide training for students and staff in the means of securing property. The Community Services Division of the University of the Florida Police Department (UPD) has many interesting presentations available to staff or student groups on a variety of security related topics.

• Contact UPD for a premise security survey. A security survey will examine an area's physical security and suggest methods of improvement.

If you have specific questions concerning office security, please contact the UPD's Community Services Division at (352) 392-1409.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology
Take a Mega-Bite Out of Computer Thefts

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>