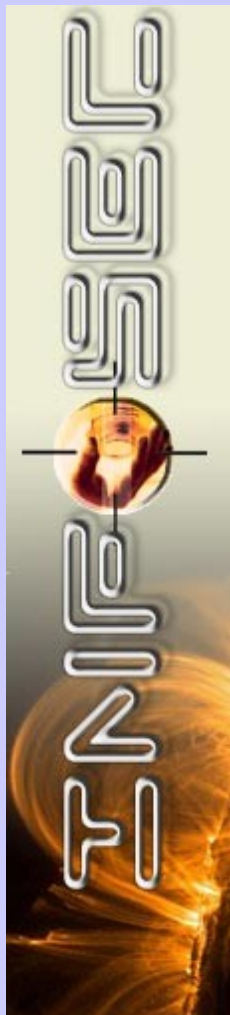




## Status of Internet Security

Click on Images for Detailed information



### Data Storage Bins Stolen from 3 Ohio Bank Branches

Police in three Ohio cities are investigating the theft of three large storage bins from bank branches earlier this month. The storage bins were used to store paper waiting to be shredded. The most puzzling part of the theft is how the thief was able to remove the bins, which were reported to weigh more than 500 pounds each. Three branches of the FirstMerit Bank in Streetsboro, Westlake and Elyria, OH each reported a bin missing beginning on October 7.

[Read More](#)

### Roane State announces 11,000 employee and student Social Security numbers stolen from employee's car

Roane State Community College has announced that the names and Social Security numbers of 9,747 current or former students were on a data storage device stolen from an employee's vehicle, along with 1,194 current/former employees' information. The Social Security numbers alone, with no names, were also stolen for 5,036 additional current or former students. The data was on a 4GB USB drive used for work-related purposes. An employee took it home October 9 to do work after hours, and left it in the car. According to a report filed by the Knox County Sheriff's Office, the employee forgot to lock the car doors.

[Read More](#)

### State Investigating Care Facility's Disposal Of Records

The Department on Aging is investigating allegations a Topeka care facility put documents with personal information in a public recycling dumpster. A person reported finding the documents Thursday night in a recycling dumpster. They say the items contained social security numbers and medical information. The incident was reported to Topeka Police and officers responded. However, TPD says it plans no further action because no laws were broken. The state, however, has regulations governing records of residents at residential health care facilities.

[Read More](#)

### Joco pub and customers were targets of credit card hacker

Llywelyn's Pub and its customers are the victims of a sophisticated cyber credit card attack, Overland Park police said Wednesday. Overland Park police encourage anyone who has used a credit card at Llywelyn's Pub within the last six months to monitor their statements for fraudulent expenses. Police Spokesman Jim Weaver said that more than 100 victims, including the owner, have been identified. They believe others could have been victimized as well. The Secret Service is working with the financial crimes team at the police department to investigate the case. Any prosecution would likely happen on a federal level.

[Read More](#)



**“Some people think technology has the answers. “**  
**- Kevin Mitnick**



### **N.Y. bank computer technician charged with ID theft**

A New York computer technician has been charged with stealing the identities of more than 150 Bank of New York Mellon employees and using them to orchestrate a scheme that netted him more than \$1.1 million, prosecutors said this week. Adeniyi Adeyemi, 27, of Brooklyn was indicted Wednesday on charges of grand larceny, identity theft and money laundering for crimes allegedly committed between Nov. 1, 2001 and April 30, 2009.

[Read More](#)

### **Leaked House Ethics document spreads on the Net via P2P**

A document containing the names of more than two dozen members of the U.S. House of Representatives who are being scrutinized for conduct violations is starting to get widely distributed over the Internet after being leaked on a peer-to-peer network earlier this week. Tiversa Inc., a Cranberry Township, Penn.-based company that offers a P2P network monitoring service said that since news of the leak broke earlier this week it has seen the file at multiple locations including London, Toronto, Washington, Los Angeles, Texas and New York. "Since this story broke we have been investigating and [have] confirmed that the file is available on P2P networks," said Scott Harrer, brand director for Tiversa.

[Read More](#)

### **Judge spanks lawyer for leaking personal details in brief**

A judge has chastised a lawyer for including the social security numbers and birthdays of 179 individuals in an electronic court brief, ordering him to pay a \$5,000 sanction and provide credit monitoring. US District Judge Michael J. Davis said he was meting out the penalty under his "inherent power," meaning no one in the court case had filed a motion requesting he do so.

[Read More](#)

### **Cable modem hacker busted by feds**

An expert on cable modem hacking has been arrested by federal authorities on computer intrusion charges. According to the U.S. Department of Justice (DOJ), Ryan Harris, 26, ran a San Diego company called TCNISO that sold customizable cable modems and software that could be used to get free Internet service or a speed boost for paying subscribers.

[Read More](#)

### **Internet Phone Systems Become the Fraudster's Tool**

Cybercriminals have found a new launching pad for their scams: the phone systems of small and medium-sized businesses across the U.S. In recent weeks, they have hacked into dozens of telephone systems across the country, using them as a way to contact unsuspecting bank customers and trick them into divulging their bank account numbers and passwords. Hackers made headlines for breaking into phone company systems more than 20 years ago -- a practice known as phreaking -- but as the traditional telephone system has become integrated with the Internet, it's creating new opportunities for fraud that are only just beginning to be understood.

[Read More](#)

## FDIC Warns Banks Of 'Money Mule' Bank Customers

The FDIC issued a warning yesterday to banks about the rise in so-called "money mules" being deployed to move money stolen via online banking. Money mules -- banking customers recruited by fraudsters to take in and transmit stolen funds -- often are hired under the guise of phony "work-at-home" schemes. As unemployment rates have climbed, so have the number of money-mule recruitment and job-related spams that prey on people losing their jobs.

[Read More](#)

## New Trojan encrypts files but leaves no ransom note

Symantec is warning about a new Trojan horse that encrypts files on compromised computers but offers no ransom note like other software designed to hold data hostage for a fee. Trojan.Ramvicrype uses the RC4 algorithm to encrypt files on systems running Windows 98, 95, XP, Windows Me, Vista, NT, Windows Server 2003 and Windows 2000, according to Symantec's Web site.

[Read More](#)

## License to Hack? - Ethical Hacking

Ethical hacking seems to be a contradiction in terms, but what better way of making enterprises pay attention to their security flaws, than by acting like criminals? To distinguish ethical hacking from the coke-fuelled, bedroom-dwelling teenage hacking of legend, it must be done in the absolute knowledge of the target, and in such a way that any resulting damage is predictable and repairable.

[Read More](#)

## E-voting system lets voters verify their ballots are counted

A new electronic voting system being used today for the first time in a government election in the U.S. will allow voters and elections auditors in Takoma Park, Md. to go online and verify whether votes have been correctly recorded. It uses cryptographic techniques to let both voters and election auditors check whether votes have been cast and counted accurately.

[Read More](#)

## Researchers Create Hypervisor-Based Tool For Blocking Rootkits

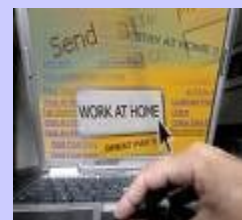
Researchers at North Carolina State University and Microsoft Research have come up with a way to combat rootkits by using the machine's own hardware-based memory protection: the so-called HookSafe tool basically protects the operating system kernel from rootkits.

[Read More](#)

## Student Blogger Case Shows That Online Anonymity Isn't Guaranteed

The anonymity of bloggers and online commentators has for the most part been protected under 1996 legislation, but a case involving a college student that criticized his dean illustrates the limits of anonymous free speech on the Internet.

[Read More](#)



*"When the economy stumbles, information is like gold." - Steve Laskey*

UC Information Security

57 Goodman Dr

Suite 400

Cincinnati, OH 45221

Phone: 513-558-ISEC

UCit Helpdesk: 513-556-HELP

E-mail: infosec@uc.edu

**Don't Miss Another Issue**

*Click here to  
Subscribe  
Now!*

**Click here to view  
back issues**

## Security Events Schedule

November

- |       |   |                  |
|-------|---|------------------|
| 3-6   | Educause 2009                               | Denver, CO       |
| 9-11  | Gartner Identity & Access Management Summit | San Diego, CA    |
| 10-13 | OWASP Application Security Conference       | Washington, D.C. |
- December
- |      |   |              |
|------|---|--------------|
| 3    | 2009 Columbus Tech-Security Conference                | Columbus, OH |
| 7-11 | 25th Annual Computer Security Applications Conference | Honolulu, HI |

### DumpSec v2.8.6

"DumpSec is my all-time favorite freeware utility," notes Jim T. DumpSec, a Windows security auditing program from SomarSoft, can produce reports on NTFS permissions for file systems, printers, shared folders, and even registry hives. It can also provide valuable information about groups, users, rights, policies, and services. "I've been using this utility for many years now, and I can't tell you how much time it's saved me," says Jim. "But more important, it's dependable and accurate."

[Download Here](#)

## SECURITY TOOLBOX



**HELPING YOU SECURE ALL  
YOUR INFORMATION ASSETS**