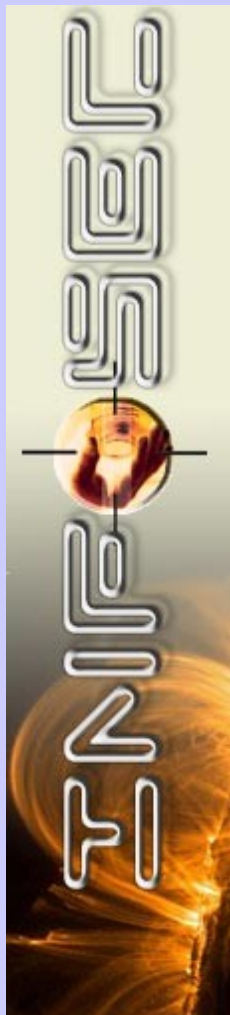




Status of Internet Security

Click on Images for Detailed information



Personal data of Cal Poly Pomona applicants inadvertently put online

The Social Security numbers, home addresses and phone contacts for at least 300 students who applied for admission to Cal Poly Pomona six years ago were unintentionally disclosed online, the university said today. The personal information, which did not include financial data, "was mistakenly put in a publicly accessible folder on a university server in November 2003," and Google and other search-engine companies mined the data, according to a statement released by Tim Lynch, senior media communications coordinator for Cal Poly Pomona.

[Read More](#)

Data breach could affect 60,000 GIs, civilians

The Corps of Engineers is investigating the recent loss of an external hard drive that could pose identify theft problems for as many as 60,000 soldiers and Army civilians. Maj. Mark Young, a Corps of Engineers spokesman in Washington, said the security breach occurred in the command's Southwestern Division, which is headquartered in Dallas, in early November. Information stored on the missing hard drive includes personal data, such as names and Social Security numbers, on a number of current and former soldiers and some civilian employees, according to information provided by the Southwest Division.

[Read More](#)

EFI victims' bank account numbers released

In the age of rampant identity theft, San Luis Obispo County officials, in a recent mailing to Estate Financial Inc. (EFI) victims, deliberately placed some investor bank account numbers on the outside of envelopes they mailed to the victims through their financial institutions. "My bank called me and said that they had received a letter from the probation department," investor Ulf Erenius said. "They were very astonished and wanted me to come pick it up. This I did and I found the most amazing thing, the county government center had put my name, bank account, and name of the bank in the address label for anyone to read."

[Read More](#)

Press Copy to have your Identity Stolen

A Call for Action investigation a year in the making reveals one possible way thieves could get a hold of your personal information. 24,000 Floridians complained to the Federal Trade Commission last year about identity theft. That made Florida the 3rd most likely place for identity theft--right behind Arizona and California. This is why the results of a WINK Call for Action investigation are so disturbing. Last year, Call for Action spent just fifty dollars to purchase ten used hard drives on eBay.

[Read More](#)



“There is no such thing as security through lack of information.”
- Emmanuel Goldstein



Hackers Breach State Database

A hacker has broken into the Nebraska Worker's Compensation database, prompting an FBI investigation and an effort to contact those who may be affected. Several thousand people could be affected by the breach, which was discovered last week when the state's chief information officer noticed an unusual amount of Internet traffic traversing the Worker's Compensation courts server. Workers who have filed court claims or who are collecting benefits may have had their names, addresses, birthdates and social security numbers compromised.

[Read More](#)

DOJ charges two programmers with aiding Madoff scheme

Two computer programmers who worked for Bernard L. Madoff Investment Securities were arrested Friday and charged in connection with the multibillion dollar Ponzi scheme run by their former boss. Jerome O'Hara and George Perez were arrested in their homes and charged with conspiracy, falsifying books and records of a broker-dealer, and falsifying books and records of an investment dealer, the U.S. Department of Justice (DOJ) said.

[Read More](#)

Boxes of medical files found abandoned

An agent with the Indiana attorney general's office removed 21 boxes of medical records from a downtown office building Friday that contain the personal information of hundreds of local people. The boxes, consisting of thousands of sheets of paper, contain patients' Social Security numbers, addresses, phone numbers, diagnoses and prescriptions.

[Read More](#)

Confidential Bushland ISD documents found

Bushland officials are wondering if an employee or an ex-employee walked out of the office with highly confidential documents. The documents were dropped off at Pronews 7 with a note claiming they were found at a recycling center in Canyon, and that Pronews 7 should investigate.

[Read More](#)

Customers' Info Stolen From Blue Cross Office

One of Tennessee's largest holders of personal information confirms that an October theft from a Chattanooga office affects about 2 million of its clients. Blue Cross Blue Shield said 68 computer hard drives that contained Social Security numbers and other sensitive information were taken from the office. When the incident occurred Oct. 2, the company told the public it didn't think there was anything personal on the hard drives, and, if there were, it would be hard to extract. The company is now sending out a letter to group administrators and brokers who sell Blue Cross Blue Shield of Tennessee insurance. The letter states: "We have confirmed that the hard drives contained encoded data recordings and certain protected health information. They may have included the member's name and ID number. It may have included the member's date of birth or Social Security Number."

[Read More](#)

T-Mobile admits employee sold private data

A employee of mobile phone operator T-Mobile is facing prosecution after selling personal details of thousands of British customers to rival companies in an alleged major breach of data protection laws.

[Read More](#)

OWASP Issues New Top 10 Web Application Security Risks List

The Open Web Application Security Project (OWASP) today released a new Top 10 list at its conference in Washington, D.C., that focuses on Web application security risks rather than the way its previous lists highlighted the most common weaknesses found in Websites.

[Read More](#)

Computer Glitch Slows U.S. Air Travel

Air travelers nationwide scrambled to revise their travel plans Thursday after an FAA computer glitch caused widespread cancellations and delays for the second time in 15 months.

The Federal Aviation Administration said the problem, which lasted about five hours, was fixed around 10 a.m., but it was unclear how long flights would continue to be affected.

[Read More](#)

DNSSEC Rollout Gains Traction

More signs that DNSSEC implementation is making inroads: The number of DNSSEC-signed zones has increased 300 percent over last year, according to a new survey, and VeriSign today announced its launch of a "boot camp" program to assist registrars, ISPs, and large registrants in deploying DNSSEC.

[Read More](#)

Fake Facebook page steals login details

A fake Facebook page which is designed to steal social networkers login details has been uncovered by PandaLabs. According to the security firm, the web page looks very similar to the real Facebook and when web users try to log-in to their account, they will be presented with an error page.

[Read More](#)

Tips For Safe Online Holiday Shopping

Cyber Monday, one of the busiest days of the year for online shopping, is quickly approaching (Nov.30), and a new survey from ISACS indicated employees plan to spend the equivalent of nearly two full work days shopping for the holidays using work computers, creating personal and business security risks.

[Read More](#)

"These are the crooks who, in the future, are going to elbow the hobbyists aside, and then settle in for a nice long vampire slurp from our e-commerce bloodstream" - Bruce Sterling



facebook

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

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

Joeware

Next to the Sysinternal utilities (e.g., PsTools), Chris L. finds that Joeware utilities are next best bet for scripting. (Note that Sysinternal utilities aren't included in this list because Microsoft acquired the company late last year.) Among the tools you'll find on the Joeware site are AdFind and AdMod (tools to query and modify Active Directory--AD) and ExchMbx (command-line tool for working with Microsoft Exchange mailboxes).

[Access Here](#)

SECURITY TOOLBOX



**HELPING YOU SECURE ALL
YOUR INFORMATION ASSETS**