Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 7
30 Γενάρη 2006

"Clean Up Your Digital Dirt Before It Trashes Your Job Search"
Computerworld (via CareerJournal.com), January 17

If you are looking for a new job, spend some time checking that any potentially embarrassing personal information (i.e. "digital dirt") has been thoroughly scrubbed from the Internet. Recruiters often have access to public information posted about job candidates using the Web, usually through search engines such as Google. In fact, according to a 2005 survey of more than 100 executive recruiters, 75% of recruiters now use search engines to uncover information about candidates, and 26% of recruiters have eliminated candidates because of information found online. Recruiters have also been known to read personal blogs and visit social networking sites in order to learn more about the personal profile of a candidate. The article includes some common tips and tricks for eliminating - or at least covering up - potentially damaging information on the Internet. The first step in cleaning up your "digital dirt" is running a quick search of your name on Google. If you find something that might impact the success of your job search, contact the site's owner and ask that it be removed. If you use a social-networking site like Facebook.com, remember that recruiters with alumni e-mail addresses sometimes log in to look up job candidates who attended the same school. Since Facebook.com members can change privacy settings so that only other students or friends can view their information, limiting recruiter access to these pages is relatively easy. It is worth the extra effort of covering up or eliminating unwanted information online. One common tactic is covering up your "digital dirt" by crowding it out with positive information. Since search engines typically rank their results based on the number of sites that link to those pages, make sure the pages you want recruiters to see have more links to them than the pages you'd rather keep hidden. You can accomplish this with a personal blog, for example. You can also monitor your Web presence through sites like Pubsub.com, which will alert you by e-mail when your name is mentioned in Internet newsgroups or on other blogs. Explains one worker who has used these tactics, "Getting regular reports on what people are saying about things related to me is really useful because a lot of times there are errors. You want to make sure you set the record straight."

"NJIT's SmartCampus Project to Create Closer Connections Among People & Places"
New Jersey Institute of Technology (01/23/06)

The New Jersey Institute of Technology is preparing to launch SmartCampus, an experimental program that will explore new ways for students to connect with each other through cell phones and other wireless devices. The program aims to link students together with shared interests and provide information about campus news and events. "We'll use mobile tracers to detect the places where students like to gather and use those places to identify students' interests and patterns", said assistant professor of information systems Quentin Jones. "SmartCampus is a unique social computing research project that uses technology to unite an urban environment - in this case the NJIT campus - into a community". The development group draws from the disciplines of electrical engineering, computer science, information systems, and human-computer interaction in an effort to cultivate personal connections and a sense of

place that could eventually change the way people interact in urban areas. The National Science Foundation is contributing $1.7 million to the SmartCampus project over the next three years, some of which will be used to provide equipment such as cell phones, laptops, and other wireless devices to program participants. SmartCampus will begin with 100 volunteers equipped with the technology to locate and interact with each other. The program will then expand to 500 participants and eventually will include the entire campus. Volunteers will have software that enables them to access a database comprised of the interests and activities of their fellow participants. The researchers are aware of the privacy and safety concerns that surround this initiative, and are requiring participants to specify which personal information they are willing to make public. Collecting geotemporal data is a central component of the project, though users can block the view of their location at certain places and times.

"Internet Coalition Sets Up Anti-'Badware' Site"
Washington Post (01/25/06) P. D4; M. Arshad

The Stop Badware Coalition, which consists of Google and institutes at Harvard and Oxford Universities, today will announce the launch of an anti-spyware campaign designed to counteract the spread of malicious computer programs that have the ability to steal personal information, spy on users who are Web surfing, and overcrowd computers with pop-up ads. The coalition will have a Web site, www.stopbadware.org, that catalogs programs that are dangerous to users so they can know if a program is harmful before downloading it. Companies that manufacture malicious software will be targeted for possible class action law suits. "For too long, unscrupulous companies have made millions of dollars infecting our computers with malicious software", says Stop Badware Coalition co-director J. Palfrey. "This is so dangerous because there are intruders in your house, but you don't know that they are in there or how they got there". Harvard Law School's Berkman Center for Internet and Society and the Oxford Internet Institute are the two main groups involved in the project, which is receiving funding from Google, Lenovo Group and Sun Microsystems. Consumer Reports WebWatch says it will be an unpaid advisor to the coalition. Google VP V. Cerf says "our interest is very strong in doing anything we can to help defend against this sort of abusive behaviour".

"Encryption Using Chaos"
Technology Review (01/24/06); K. Greene

Security researchers are exploring a new method of encryption where the chaotic fluctuations of a laser beam encode messages passing over fiber optic cable, which require a receiving laser of almost identical properties to decode it. The University of the Balearic Islands' C. Mirasso used chaotic laser encryption to transmit data at 1 Gbps, a speed equivalent to the typical commercial transmission rate. To transmit data inside a chaotic laser, the message must first be translated into an optical signal, which is then funneled into the laser that emits it along with its beam. The chaos of the beam is then accentuated, and the message is transmitted to a receiving beam of near-identical properties. Upon receipt of the message, the process gives way to chaotic synchronization, which, while still not completely understood, pairs the sending and receiving lasers together, and the receiving laser subtracts the chaos of the transmission to recover the original message. Chaotic laser encryption will have to prove its effectiveness if it is to supplant conventional optical signals, though a body of scientists has already reported the successful transmission of a chaos-encrypted message through an intermediate laser, which is critical for commercial applications where messages would have to travel great distances. While Mirasso admits that the basic technology is not perfect, he will next

turn his attention to developing smaller devices for communication based on chaotic encryption, though he does not expect commercial applications of the technology to appear for the next five years.

"Privacy for People Who Don't Show Their Navels"
New York Times (01/25/06) P. 7; J. D. Glater

There is growing interest today in software that protects the confidentiality of Internet users sending emails and posting blogs. Tor, a free anonymity software package, has seen increased downloads, while the free Java Anonymous Proxy is another program for users who want to communicate anonymously. While it is difficult to quantify how many people have opted to conceal their Internet presence, the recent surge in Web anonymity can be attributed to a growing number of users who want to download music but are concerned about legal reprisals from the entertainment industry, as well as those who use the Internet as a confessional or a forum for political dissent. Electronic Frontier Foundation technology manager C. Palmer says, "People in the world are more interested in anonymity now than they were in the 1990s". While many software companies are moving away from identity protection software, their heavy investment in the technology several years ago preceded demand, as a rapidly growing number of Internet users is growing concerned with hackers looking to steal credit card numbers, bank accounts, and other sensitive personal information. Despite the renewed interest, many identity protection ventures are still having difficulty turning a profit. Tor's Defence Department funding has run out, and project leader Roger Dingledine is now working without compensation as he searches for new backers. Tor employs a technique called onion routing where a tiered server structure extricates the user from the sites he has visited. The Privoxy software that comes with Tor prevents new cookies from being created and blocks a computer from sending some personal information to Web sites, though the package can slow browsing speeds.

NSA Spy Program Hinges on State-of-the-Art Technology"
National Journal (01/20/06) Vol. 38, No. 3, P. 47; S. Harris

Cutting-edge data-mining technologies play a key role in the National Security Agency's (NSA) plan to collect and analyse vast volumes of call and email traffic to extract valuable data about terrorists and other potential enemies. Data-mining not only spots key words but also unearths hidden relationships between data points, and can even identify the thinking patterns and biases of specific analysts and propose alternative speculations. In 2002, the Advanced Research and Development Activity (ARDA) group apportioned $64 million in research contracts for the Novel Intelligence from Massive Data (NIMD) project, a program to develop an early-warning system designed to prevent information overload--and thus the overlooking of important data--among intelligence analysts. A "Call for 2005 Challenge Workshop Proposals" issued by ARDA says research funded by NIMD is supposed to not only help analysts cope with the flood of data, but also to "detect early indicators of strategic surprise, and avoid analytic errors." The NIMD project and other ARDA-supported efforts are very similar to the Defence Department's Total Information Awareness (TIA) program, which sought to establish a system for uncovering terrorist plots by mining intelligence databases as well as private databases; concerns over TIA's potential to infringe on civil liberties led to the program's suspension in 2003, but other agencies are continuing the development of tools used in TIA. Also generating discomfort among lawmakers is the unanswered question as to whether NSA's current data-mining programs, like TIA, are making sizable investments in technology and policy research to safeguard privacy. Former program manager in

the office of ex-TIA manager John Poindexter Tom Armour confirms that the NSA's interest in pursuing projects such as NIMD lies in the analysis of call and email traffic.

Expert Calls for Increased E-Voting Security"
Computerworld (01/23/06) P. 14; M. Songini

In a Q&A with Computerworld, security specialist Herbert Thompson describes his volunteer effort to hack into Diebold Elections Systems' e-voting machines in Leon County, Fla., on Dec. 13, in response to fears about accuracy and security expressed by local officials. Thompson, director of research at Security Innovations in Wilmington, Mass., says he wrote a five-line script in Visual Basic that provided access to the central tabulator of the Diebold AccuVote optical scan device, and the opportunity to change votes without leaving a log. He added that Finnish security expert H. Hursti was able to change the content of a memory card, describing his effort as the equivalent of stuffing a ballot box. As a security expert, Thompson views the issue more as a bad software matter than as a political one. He says the exercise was not about Diebold, because other vendors are also making tabulation software and optical scan gear that is not open to independent audit and analysis. Thompson says the security of e-voting pales in comparison to the standards of critical business processes. "There should be much more severe security-testing requirements", he says. "The key is you need to raise awareness that these vulnerabilities do exist and can be exploited, and you need a way of measuring security".

"Torvalds: No GPL 3 for Linux"
CNet (01/26/06); S. Shankland

Voicing objections to the digital rights management clauses in the recently released draft for GPL 3, L. Torvalds rejected the first update to the license in 15 years. "I think it's insane to require people to make their private signing keys available, for example", Torvalds said of the language in the update opposing digital rights management. The rift is symbolic of a long-standing philosophical difference between the pragmatic Torvalds, who has made many concessions to proprietary models over the years, and Free Software Foundation (FSF) founder R. Stallman, who remains dogged in his ideological adherence to the ethical and social equity of free software. Torvalds wrote in 2003 that while he may not be a fan of digital right management personally, he feels that users should be able to apply Linux to any end that they see fit. Torvalds is adamant that a license should simply serve to keep source code open, and that any additional provisions unnecessarily extend its scope. Much of the controversy surrounding GPL 3 revolves around copyrights, as MySQL, OpenSolaris, and several other open-source projects require that developers relinquish copyrights to the main organizing body, while Linux keeps copyrights decentralized. The FSF's Eben Moglen has also taken issue with Torvalds for employing proprietary video drivers, claiming that he uses an impure version of the license. Some analysts believe that by rejecting GPL 3, however, Torvalds is missing out on some of the improvements that the update has to offer.

"In Case About Google's Secrets, Yours Are Safe"
New York Times (01/26/06) P. A1; A. Liptak

Google's resistance to a US federal subpoena for a sample of 1 million search results is raising profound legal arguments about trade secrets and privacy now that the government has taken Google to court over it. The US government is asking for search results stripped of personal identifying information, and though MSN, Yahoo!, and AOL already have complied,

Google has balked by arguing that revealing its search results in response to a vague and broad subpoena would compromise Google's trade secrets. Google's policy is to comply with "valid legal process;" for example, AOL itself receives about 1,000 subpoenas per month from cases involving divorce, fraud, and other criminal matters. Google also asserts that complying with this request would torpedo its commercial reputation, and on the sidelines privacy advocates fear the US government one day may amass personal profiles based on peoples' varied and revealing Internet habits. The government, in a case unrelated to its security-minded data mining program and national eavesdropping without warrants, is collecting search information in order to attempt to prove in court that search engine filters are not enough to protect children. The government is concerned with banning "material that is harmful to minors" in accordance with the 1998 Child Online Protection Act. However, this law has never been enforced because a Philadelphia court has enjoined it, and in 2004 the Supreme Court upheld that injunction, but left the question of filter technology open. The government is seeking search engine results in order to prove that filters do not work.

"Senate Committee Considers Broadcast Flags to Combat Piracy"
Medill News Service (01/25/06); M. Bell

The Senate Commerce Committee is debating legislation that would permit broadcasters to prevent certain programs from being recorded in an attempt to curb media piracy. A federal appeals court struck down the FCC's mandate of broadcast rules flag last year, ruling that the agency had overstepped its bounds by allowing broadcasters to encrypt their programming so that digital recording devices would be unable to record the content. Consumer groups argue that the broadcast flag is unfairly restrictive of noncommercial uses of programming, while broadcasters claim that it is an essential mechanism to counter piracy. Broadcasters presented the committee with the gloomy prospect of quality content migrating to cable networks, which have the right to flag programming, if they were not able to block multiple retransmissions. The American Library Association's J. Brand calls the broadcast flag "detrimental to the public," since it makes it illegal to retransmit copyrighted works over the Internet for educational use. Consumer advocates say the restrictions will be tantamount to censorship, as many innocent and legitimate applications of retransmitted television content, such as its use in schools and in civic discourse, will be short-circuited. Officials from the music industry also support the legislation, arguing that new digital radio services put their industry more at risk than television. Still, the audio flag does not enjoy the broad coalition of support that the television industry has demonstrated for the video flag, which is now favored by manufacturers, broadcasters, and content providers alike. Sen. T. Stevens (R-Alaska), who chairs the Commerce Committee, has said that the bill needs some modification before it is turned over to the floor for a vote, and manufacturers are pressing for at least 18 months lead time to incorporate the flag into new devices if the bill passes.

"Sensors Detect Icy Bridges"
United Press International (01/17/06); G. Koprowski

Researchers are hopeful that tiny wireless sensors will significantly improve public safety, as the developing technology could be used to alert authorities to the impending collapse of a bridge or dangerous seismic activity along a fault line that could be an indicator of an earthquake. Clemson researchers are placing small wireless devices called motes on roads and bridges to notify authorities when they begin to approach their structural stress point, or breaking point. The network of motes monitors light, sound, temperature, humidity, and other factors and relays the data back to computers for analysis. Clemson computer-science resear-

cher J. Hallstrom and his team have created a test-bed wireless sensor network for other researchers to try out their own technologies. B. Kasanoff, president of Now Possible, maintains that with an estimated 1 trillion sensors in existence, government authorities would be negligent not to use them to improve the safety of public infrastructure. Kasanoff predicts a proliferation of sensors on roads that will glow to indicate icy conditions, cameras and sensors that would issue a court summons to any car or truck that exceeds the posted weight limit of a bridge, and sensors at beaches to monitor for pollution. The Incorporated Research Institutions for Seismology (IRIS) is distributing wireless modems throughout the country to record seismographic data that will be used to analyze the physics and processes of earthquakes and volcanoes. The data will be recorded in a shared database to build on scientists' understanding of the interior of the earth. By placing wireless sensors in remote areas where there is no landline telephony, the IRIS project will greatly increase the geographic scope of seismic research. Bluetooth will also have a major impact on seismography, particularly when it melds with Ultra-WideBand technologies.

“The Search Continues"
Government Computer News (01/23/06) Vol. 25, No. 2; B. Grimes

In a recent interview, Internet pioneer V. Cerf shared his thoughts on the state of the network that he helped create. While with R. Kahn on ARPANET in the early 1970s, and later at DARPA, Cerf had a basic idea of the how the network would operate, though he did not envision its evolution to the scale on which it is used today. As Google's chief Internet evangelist, Cerf is devoted to bringing the Internet to the 5.5 billion people who are not currently using it, as well as traveling to Google's engineering facilities throughout the world to nurture the culture of ideas and innovation. Google has also created a small operation in Washington, DC, to work with legislators and the Library of Congress to make more government information available through Google search technologies. Cerf credits the use of metadata as complementary to Google's search strategies, which is beginning to use indicators from XML and other databases to generate better search results. Cerf looks forward to the implementation of IPv6, which he expects to enable a far greater number of devices to tap into the Internet without requiring Network Address Translation (NAT), though he acknowledges that NAT is a useful security mechanism for authenticating end-to-end interactions. Cerf credits ICANN as a reasonably functional institution, considering the hundreds of thousands of users that it brings together in a cohesive system, though many security and usability issues, such as spam, intellectual property, DoS attacks, and viruses are beyond the governing body's scope. While Cerf believes that ICANN is overseeing its portion of the Internet's development ably, he welcomes the creation of the Internet Governance Forum at last November's World Summit on the Information Society. Google and VoIP are among the Web's most impressive developments, though Cerf believes that "99% of the Internet's applications have yet to be invented".