

If you are having trouble viewing this email, please click [here](#)



ua.InfoSec Monthly Update

October 2009

Sec-U-R-IT-y Tips | Security Concerns Regarding Peer-to-Peer (P2P) File Sharing

Peer-to-peer (P2P) networking has become a popular method for sharing files, music, photographs and other information. P2P allows computer users, utilizing the same P2P software, to connect with each other and directly access files from one another's hard drives.

Although file sharing seems benign in concept, there are a number of risks associated with it. Read about the risks at <http://security.arizona.edu/files/oct2009securitytip.pdf>.

Securing UA | Security Awareness Day 2009: Security on a Shoestring

Bringing security awareness to UA employees and the community is a significant goal of UA InfoSec. The University of Arizona's 2009 Security Awareness Day will be held on Friday, October 16, 2009, during Family Weekend. Why pay through the nose to secure your computer and data? Visit InfoSec's tent on the UA Mall for information security advice, tools and techniques for any budget. Security Awareness Day is a free event, open to the public.

News | Online Hucksters Bought Malvertising Space Directly From New York Times

Recently, criminals bought advertising space on the New York Times website directly from the newspaper. Posing as a legitimate company, they persuaded NYTimes.com to run online ads that initially appeared as legitimate before being switched to an image showing a "scan" for computer viruses. Visitors were then advised to buy phony antivirus software to fix the problem. For more on this increasingly common approach of online criminals, view the full article at

http://www.nytimes.com/2009/09/15/technology/internet/15adco.html?_r=2.

News | Trend Micro Study Finds Malware Often Remains for Months

A study from Trend Micro found that malware sticks around on computers it infects. Of 100 million IP addresses studied, 80% that had been infected remained infected 30 days later; 50% remained infected 10 months later. To read about these malware infection trends, go to

<http://www.scmagazineus.com/Study-Malware-persists-on-compromised-machines/article/149089/>.

Internet users can minimize their risk of exposure to malware by using security software and content inspectors and by installing critical security patches for software. For tips on these tools and techniques, see steps 1, 2, 3 and 9 at <http://security.arizona.edu/topten>.

Tools | Norton Safe Web

Everyone knows that the Internet is huge, with many online threats like viruses, phishing, and spyware, and a lot of unsavory websites—websites that will try to deceive you, steal your credit card numbers or passwords, or even crash your computer. For a quick check on the safety rating of a website without the hassle of software download or registration, go to <http://safeweb.norton.com>.

[InfoSec Web Site](#) | [Contact Us](#)

InfoSec Monthly Update is distributed by
Information Security Liaisons for the
University Information Security Office
1077 N. Highland Avenue, Tucson, Arizona 85721
tel: 520-621-UIISO | fax: 520-621-9222
iso@u.arizona.edu

© 2008 Arizona Board of Regents