

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



ua.InfoSec Monthly Update

February 2009

Alert | Malicious Software Alert

Malicious computer software known as Conficker or Downadup has infected millions of computers worldwide and is gaining momentum. Some of the infections have occurred at The University of Arizona. Nearly all Microsoft Windows-powered computers can be compromised by Conficker. Computer security researchers expect that Conficker will enable unauthorized people to gain control of infected computers and the data on them.

Conficker spreads in several ways. If an infected computer is connected to a network, Conficker will immediately scan the network looking for a particular vulnerability and use it to gain access to another Windows computer. It can also gain access to a networked computer by guessing the password. Lastly, it can copy itself to any removable USB-based device, such as a flash drive or camera. It is then executed when inserted in another computer that has been configured to automatically play USB-based devices. This flexibility means that more than one defensive measure is needed to minimize the risk of infection.

Windows users should implement the defensive measures listed on the Information Security web site, <http://security.arizona.edu/conficker>. The site includes links to instructions and tools. If you have a local IT support person, check with him or her before implementing any of these suggestions on a UA-owned computer. Otherwise, contact the 24/7 IT Support Center, <http://the247.arizona.edu>, if you need assistance.

News | The President and His BlackBerry

Compromise Allows Obama To Keep BlackBerry

by [Laura Sydell](#)

Morning Edition, January 23, 2009 · Barack Obama is the first president to have a BlackBerry, even though it makes security officials nervous. During the campaign, Obama and his BlackBerry could not be parted. The president and his personal digital assistant will stay together with some changes.

<http://www.npr.org/templates/player/mediaPlayer.html?action=1&t=1&islist=false&id=99790788&m=99790766>

Sec-U-R-IT-y Tips | Challenge or Secret Questions

Knowledge-based authentication or the use of "Challenge or Secret Questions" helps computer users access their accounts when they forget their password. The questions are often designed as simple, easy to-remember "prompts" that only the authorized user should be able to answer. They are in effect a backup to your password. To read more, go to

<http://www.security.arizona.edu/files/challengequestions.pdf>.

[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