



Take a second to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: www.longwood.edu/infosec

May 2009



What is pod slurping?

Pod slurping occurs when a portable storage device like a PDA, iPod, thumb drive or external hard drive is connected to an unattended computer by a malicious intruder to steal data.

Pod slurping is a new term in MOAT 2009!

What Juicy Details Are in Your E-mails?

While you may at times be tempted to think no one would be interested in reading your e-mail, you should consider what a treasure trove of life's little details your e-mail account can be. Actress Salma Hayek recently learned this lesson the hard way when her e-mail account was hacked due to weak security questions which resulted in her love of Japanese face massages being revealed to the world. (This is the same way that Sarah Palin's personal e-mail account was hacked last year. See the [January 2009](#) edition of *The Security Minute*.)

The gossip blogs didn't find anything too juicy in Hayek's e-mail account; however, the information uncovered could have been exploited to endanger her personal safety or to perpetuate further fraud against her.

Among the information found within Hayek's e-mail account:

- The billing address, phone number, expiration date and the final 4 digits of the account number of the credit card used to pay for the e-mail service
- Travel confirmation information
- Listings of Apple I-Phone Apps that she had downloaded
- Names and addresses of her frequent contacts, such as assistants
- Her communications with fashion designers
- Japanese face massage appointment information

Does your e-mail account at home or at work contain similar information?

Choosing difficult to guess passwords and security questions and keeping that information private is important in protecting yourself from prying eyes. As Hayek's case demonstrates, while information security practices are in place to protect our personal information (credit card numbers, Social Security numbers, etc.) and the personal information of others, there are also many mundane details of our daily lives that we would not want others to know.

What Happened to the Conficker Worm?

As April 1 approached all computer users were eagerly anticipating the potential impact of the Conficker worm. April 1 passed without noticeable impact from the malware. Did you think the worm was just hype? While nothing extraordinary happened on April 1, a month later computers worldwide are still infected with Conficker. Some of those infected computers have been used as part of a spamming campaign and others have been plagued by scareware. Scareware is fake antivirus software that users are prompted to buy from pop-up ads that claim the computer is infected. The infections the pop-up ads claim to find aren't real and neither are the products that claim to remove the infections.

Conficker infected computers that did not have up-to-date Microsoft patches or antivirus software. One sign of infection from Conficker, and other malware, is antivirus software that has been deactivated. Always make sure your antivirus software is up-to-date and working properly at home and at work!

To confirm that your McAfee software is up-to-date you should right click on the V-Shield icon in the bottom right hand side of your screen (next to the time) and choose "About VirusScan Enterprise". The "DAT Created On" date should be no more than a few days old. Visit the Information Security web site to learn how to update your DAT files: <http://www.longwood.edu/infosec/antivirus.htm>



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. If you have any questions regarding the newsletter, please contact Melissa Short at 434-395-2034 or shortmj@longwood.edu.