How the University Protects your Computer and Data

How the University Protects Your Computer and Data And Your Role in the Process

The Threat: Crypto Ransomware

You may be familiar with an emerging threat where cyber thieves encrypt all the files on your hard drive (and network shares), and demand a ransom payment in exchange for the key that will restore your files [1]. I read recently about just such an attack that uses ads displayed on legitimate web pages. When clicked, the ads will redirect visitors to a site that attempts to exploit unpatched versions of Adobe's Flash software, and install the encryption malware on your computer.

In such a scenario, antivirus will not protect your system or your information.

There are two important lessons in this story.

- First, you cannot predict when you may be exposed to an attack from the Internet.
- Second, if your system is not fully patched, that exposure will result in successful exploitation of your system by an attacker.

UAlbany's Patching Process

On the second Tuesday of every month, Microsoft issues security and stability updates for its software, both the operating system and applications like Word, Excel, Internet Explorer, etc. Additional security updates are released by Adobe (Flash, Reader), Oracle (Java), and browser publishers like Mozilla (Firefox) and Google (Chrome).

Updates for the campus anti-virus software (SCEP) are also released on a more frequent basis.

The University rolls all these updates into deployment packages that can be distributed to faculty and staff desktop machines by your local Technology Coordinator, e.g., CAS Computing.

Your Part

The campus has the capability of delivering these updates to your machine, but you have to complete the final step for the updates to take effect. This entails doing the following:

Shutting your computer down completely and restarting it.

The timing of this action is left to your discretion. However, the sooner; the better. At the very least, you should reboot your machine within a week of the patches being deployed. Failure to do so leaves your computer, and your data, unprotected.

[1] http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html

Need more help? Submit an ITS Service Desk Request.