

Software Updates

Did you know that most UMASSMED Domain Member systems are automatically updated?



System Updates are frequently released by software vendors in order to keep their applications secure. Operating system software and other applications software

Systems must be frequently updated in order to avoid being compromised

need to be updated on a regular basis to patch loopholes and other vulnerabilities which are not found during application development. All the applications on the laptop should be patched and updated from appropriate vendor's website.



Information Services Department
Information Security Office
55 Lake Avenue North
Worcester, MA 01655

Phone: 508-856-8643
Fax: 508-856-5150
E-mail: ITsecurity@umassmed.edu
Web: <http://www.umassmed.edu/IS/ITsecurity>

University of Massachusetts Medical School

Information Security Awareness Series

Application and System Updates



Security Starts with Awareness for Everyone

October is National Cyber Security Awareness Month

Topic of the Week: Software Updates

Frequent software updates is an effective way to insulate computing systems from most “malware”



Keep your Systems current

The best known forms of Malware are worms and viruses. Malware is software designed to infiltrate or damage a computer system, without the owner’s informed consent.

Today’s Malware includes worms, viruses, spyware, rootkits, backdoors, Trojan horses, keystroke loggers and so on. There is an active community of criminal hackers who seek to load Malware onto computing systems by leveraging vulnerabilities in Operating Systems (Windows, Mac OS, etc.) and Applications. This is an arms-race of sorts, between the criminal hacker community and the software vendors.

During the 1980’s and 1990’s it was usually taken for granted that malicious programs were a form of prank or vandalism. In recent years the greater portion of malware has been written with profit motives in mind.

Frequently Apply Updates

The most effective way to remain unaffected by the endless stream of current malware attacks is to update your operating system, applications and anti-virus signatures regularly.

Powerful new exploits are being released at a quickening pace. Apply-



ing updates or patches on a monthly or weekly basis is often inadequate. Systems must be patched on a daily basis. This is most important for systems that are not centrally maintained and which do not receive the benefit of automated updates as delivered by Information Services.

Independently maintained and non Domain member machines should be configured to update themselves (anti-virus and operating system) updates on a daily basis.

Automatic Updates

- Configure your anti-virus software to update it’s signature file on a daily basis (this is automatic with supported UMASSMED domain systems). The Desktop Services section of the IS Web Site can show you how.
- If possible, configure your operating system to make a daily check for updates (this is automatic with supported UMASS-MED domain systems).



Information Services Department
Information Security Office

Phone: 508-856-8643

Fax: 508-856-5150

E-mail: ITsecurity@umassmed.edu

Web: <http://www.umassmed.edu/IS/ITsecurity>