Please forward to all faculty and staff.

Dear Colleagues,

The UM Information Technology Security Services (ITSS) Office has informed me that the campus network receives about 30 network attacks per hour and up to 30,000 network attacks per month. Some of these attacks are successful, resulting in hundreds of compromised desktop computers per month. Other universities—most recently, Ohio University and the University of Texas at Austin—have reported data thefts from compromised computers that have exposed personal information such as names, social security numbers, and even medical information for faculty, staff, and students.

http://www.ohio.edu/datasecurity/
http://www.mccombs.utexas.edu/datatheft/release_4.23.06.asp

In order to prevent a similar security breach in LSA, I have asked LSAIT to expand its preventative measures to protect our computer systems. As you will recall, last summer I asked LSAIT to begin a comprehensive effort to improve the College's computer security posture. This initiative was a response to increased concerns about the vulnerability of the University network, our individual machines, and the data that resides on them. The University's Standard Practice Guide (SPG601.07) and good stewardship of our resources and intellectual work make it incumbent upon us to do all that we can, consistent with our mission and the principle of academic freedom, to make our information technology environment as secure as possible.

To accomplish this, LSAIT scans our network monthly to identify insecure or outdated systems that, if compromised, could pose a security risk to the computer and, potentially, the community as a whole. As we all know, computer security has a continuing evolving landscape and requires a security effort that can respond to "threat changes" and "technological advances." At the time of our initial communication last year, I identified a follow-on effort to institute standards for minimum baseline version levels for operating systems (OS) and server applications for all computers that connect to the LSA Network. We are now proceeding with this part of our security initiative.

I want to reiterate that this initiative is a cooperative endeavor. LSAIT will continue to work with individuals and unit computer support staff to minimize any disruption that upgrading to a new operating system can cause. In the rare case where equipment or software cannot be upgraded to meet the minimal version standards, LSAIT will work with you to secure that system by putting it behind firewalls and/or implementing other mechanisms for protecting the machine and the network from potential exploits. I am sure that all of us are well aware of the risk to the entire University community when there are computers on the network that are vulnerable to malicious computer activity.

Please take a moment to read the attached security document provided by LSAIT. This document outlines the process by which the College intends to secure, as tightly as possible, both the workstations and, by extension, the network that we all share. It includes a table for the Minimum Standards for OS and applications that the College will require all workstations to meet by January 1, 2007. As always, LSAIT will work with you and your staff to ensure that these standards are met and to address situations that limit your ability to bring a system into compliance. As you'd expect, the standards for computer security will evolve over time as new systems, software, and threats develop. We ask that you assist your computer staff as they work to ensure that all of your computer systems are protected.

Especially in the open environment of a University, there is always the need to strike a balance between increased security and complete openness. It is unfortunate, but unavoidable given the significant dangers we face from the open Internet, that we need to tighten our computing security standards. I trust that you understand that this undertaking is necessary to protect our intellectual property, sensitive institutional and personal data, and to ensure a reliable and secure computing environment for all.

Terry

Terrence J. McDonald
Arthur F. Thurnau Professor,
Professor of History, and Dean
College of Literature, Science, and the Arts

2005 LSA Building
734-615-8360
FAX: 734-764-2697