

-----Original Message-----

From: NAKASHIGE, JOCELYN

Sent: Thursday, September 18, 2003 3:16 PM

To: UCSFSTAFF@ITSSRV1.UCSF.EDU

Subject: IT Security Update

---FORWARDED ON BEHALF OF VICE CHANCELLOR STEVE BARCLAY---

TO ALL FACULTY, STAFF AND STUDENTS

Subject: IT Security Update

In recent weeks UCSF has suffered significant disruption of essential operations due to attacks on our computer systems by viruses and worms that took advantage of known vulnerabilities in the so-called Microsoft Windows operating system. These particularly powerful computer infections, once in place, spread quickly and easily from one UCSF computer to another sending copious amounts of infected email, degrading computer and server performance, bringing down the network, and disrupting normal academic, clinical, research, and administrative operations.

Several realities emerge from these events:

- This disruption could have been minimized or possibly even prevented. Software patches that would have blocked the virus and worm attacks were available but had not been installed on many UCSF computers running Windows.
- Protecting ourselves will require increased preparation, vigilance and collaboration between Campus IT, the Schools, and the Medical Center.
- The UCSF network and technology infrastructure will be attacked again.

UCSF campus and medical center information technology (IT) units, with guidance from the Chancellor's IT Governance Committee, are working on a plan embodying both short- and long-term strategies to put in place an information security structure to address this increasing threat to mission-critical systems and functions.

Short-Term Actions

To immediately address current threats, the following actions are being taken:

- Recruitment of two senior network security specialists - (Hiring process began months ago, start dates will be in October)
- Installation of Network Traffic Analysis Tools (to be accomplished this Fall) that
 - provide better visibility of the level and types of network traffic at the network connection level
 - allow better detection and targeting of specific problem devices
- In emergency situations, network access to any computer found to be infected or that poses an immediate threat to the network will be denied. Until the tools above are available it may still be necessary to shut down individual subnets but only under the direst of circumstances. This action will only be taken under the direction of the Campus and Medical Center CIOs, following agreed upon policies and procedures, and after thorough analysis by a team of Network Operations Center staff. Immediate notification to affected individuals or units will be undertaken.

- Establishment of an improved desktop support framework with better lines of communication between distributed IT support personnel and central IT units. The first step in this process, to be made in consultation with departmental managers and IT technicians, will be an assessment of the capabilities of the existing support structure and an identification of the gaps in support and developing a plan to close them.

The above actions represent improvements, but preventing future attacks will require everyone's diligence. Central and departmental IT staffs need the cooperation of all computer users to keep current with software security patches, install anti-virus software, and consider installing personal firewalls where appropriate. Despite numerous communications to the IT support community many computers on campus today still remain "unpatched" and vulnerable.

Long-Term Actions

Over the last few months, the central IT units have been developing a strategic action plan to improve the level of information security on an enterprise-wide level. This includes major improvements to perimeter security, the purchase of additional software security tools that identify - and prevent - attempts to hack into the network, and the implementation of secure messaging. This planning is being undertaken in a careful, methodical manner and will include solicitation of input from the user community through the IT Governance process and consultations with campus and departmental leaders.

In addition, we will provide periodic updates on the activities outlined above to the UCSF community.

For additional information on security patches, personal firewalls, antivirus software, and other security-related items, please see <http://isecurity.ucsf.edu>. If you have questions about how to keep your computer system protected, contact your Computer Support Coordinator (CSC). If you don't have a CSC, contact Customer Support Services at 514-4100.

Questions and comments can be directed to Ian Tuller, Director of Customer Support, Security and Planning at <mailto:feedback@its.ucsf.edu>.