

**MACALESTER COLLEGE**  
**INFORMATION TECHNOLOGY SERVICES**

“Compromised” computers have been infected by threatening worms or viruses, or have been hacked. Compromised computers pose a threat to all other computers sharing the College network by emitting interfering data and/or retransmitting worms and viruses. Computers can be compromised without the user’s knowledge, if preventive software patches and anti-virus updates are not regularly applied. Because a single compromised computer can cause so many serious problems for all others on our network, we must respond quickly and thoroughly when a compromised computer is identified.

**RESPONSE TO COMPROMISED COMPUTERS**

1. Network or other ITS staff members identify an IP address that is infected with a worm or virus, or otherwise is compromised and threatens other network users.
2. Network staff identify the problematic computer in the network registration system and discover the name of its registered owner. Network staff blocks the computer’s network access. Because of the threat to others posed by compromised computers, network access blocking must occur immediately. Any attempt to access the Web will lead to a page informing the student of the circumstances and referring the student to the Help Desk. Attempts to access resources other than the Web will fail.
3. If the student calls the Help Desk, ITS staff members explain the circumstances, and counsel the student on fixing the problem.
4. Help Desk staff notify Network staff when it is safe to restore network access.

Created July 2004; revised July 2007