Stony Brook University
Computer Science

Guidelines on User Security Awareness

CS Department Guidelines on User Security Awareness

Recommended processes to keep users and staff aware of security issues:

The annual Start of Semester (SOS) meeting is an ideal time to bring security awareness to the forefront.

1. Review *Acceptable Use Policy, Password Policy, Dial-in Access Policy, Audit Policy and Antivirus Policy*
2. Discuss impact of security breaches to the CS department
3. Be sure students are aware of the fact that home systems "on" the internet are able to be attacked

After testing (cracking) user accounts a general email to users that accounts have been cracked and disabled will re-enforce good password habits

The CS department FAQ's covering *Securing Your System* should be kept up to date and when additions are made they need to be announced on the site splash page

Since Windows virus come out at regular intervals they present a useful excuse to re-point users attention to security and department web content on security issues.

Remind the program director assistants that new students are required to read the department *Acceptable Use Policy* **prior** to receiving their account information.

New secretarial help should be brought up-to-date with department security policy and general security awareness. The secretary's supervisor should bring the security issue up as part of showing the new person their duties and procedures. Security awareness is just another procedure.

The Director of Labs should meet new faculty and as part of their "tour" of the department a discussion of security policies should occur

When faculty establish labs the Director of Labs should review security policy as it affects the lab and its' users

Lab Managers and System Staff supervisors should always raise the question of security impact when any new service, OS upgrade or lab is being discussed with faculty or Staff associates. Keeping secure systems is job one.

Staff members should receive positive reinforcement when they raise security issues or make others aware of new vulnerabilities or tools to secure systems.

A consistent, systematic approach to configuring facilities with security issues in mind instills the import of security in the Staff's work.

Consistent reaction to policy violations will "program" the user community to pay heed to department security policies. Exceptions raise doubts or add confusion as to how important policy really is. It's important.