Security Awareness

Computer and Information Security at SPU

Protecting the network and its users from viruses and malicious activity is an on-going process on the part of both CIS and each user of the network. Security affects everyone's privacy and ability to use the network. Effective security involves both sound technology and user awareness and education.

Core Network Services and Servers

SPU deploys many measures to minimize security risks to date, including keeping core servers up-to-date with the latest security software, maintaining firewalls at key locations within the network, and actively monitoring systems and usage for abuse and/or malicious behavior.

Desktop and Laptop Computers

For systems owned by the university, device health requirements are enforced automatically through Active Directory group policy.

For personal devices, security is in the hands of each user. Personal systems should be:

- current with all **operating system updates**;
- running an active **anti-virus** program;
- periodically **scanning for and removing spyware**; and
- using a local desktop **firewall**.

See **System Health Requirements** for more information on meeting the above requirements.

Report a Problem or Concern

CIS will only request passwords over the phone or in-person - **never** give your password or other personally identifiable information out in an email communication.

Related articles

- Password Best Practices
- Downstream Data and Sensitive Private Information
- Determine a Computer is Infected
- Viruses and Malware
- Security Awareness