



PRIVACY. RESEARCH. HOMEWORK. REPUTATION.

You can lose them all at the touch of a button. Students, faculty, and staff are all potential victims of computer crime. Personal computers are as much at risk as larger servers. Although day-to-day computer use is usually uneventful, disagreeable incidents that could have been prevented are happening frequently. Please spend the next few minutes carefully reading this material, as it may prevent you from becoming the next victim. Just as highways make interstate crime easier, networking can bring “inter-computer” crime right to our desktops. Today, 300 million people can touch our computers with the click of a mouse. They can use the power of today’s computers to automate and assist criminal behavior just as we use that power for our benefit. Threats aren’t always from the outside. We can hurt ourselves by mishandling our own information or that of others. Our own errors can be just as bad as a computer virus or a computer hacker breaking in and wreaking havoc.

INFORMATION TECHNOLOGY SECURITY OFFICE MISSION

The IT security coordinator concentrates on university-wide security issues, spanning the diverse and decentralized computing environment. Key objectives include assessing risk, developing disaster response plans, establishing strategic direction, defining policy, tracking security incidents, following state and federal guidelines, and cultivating IT security awareness by coordinating training and educational opportunities for the George Mason community.

ADDITIONAL RESOURCES THAT SUPPORT INFORMATION TECHNOLOGY SECURITY EFFORTS


ITU Support	http://itusupport.gmu.edu
Student Technology Guide	http://itu.gmu.edu/pdf/stu_techguide.pdf
Security Review Panel	http://www.gmu.edu/srp
Copyright Office	http://library.gmu.edu/copyright/
Campus Police	http://www.gmu.edu/police/chief.html
EDUCATIONAL PROGRAMS AND CENTERS	
Bachelor of Science in IT	http://ite.gmu.edu/bsit/
Center for Secure Information Systems	http://ise.gmu.edu/~csis/intro.html
Critical Infrastructure Protection Project	http://www.gmu.edu/departments/law Search for “CIP”



<http://itu.gmu.edu/security>

George Mason University

WHAT YOU CAN DO TO MINIMIZE IT SECURITY RISKS

- Read and adhere to the Responsible Use of Computing Policy 1301. See <http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html>.
- Create strong passwords. Avoid words found in the dictionary, use mixed case, be creative. Suggestions and guidelines can be found at <http://itu.gmu.edu/security/practices/guidelines.html>.
- Use and keep current antivirus software, available to students and staff on the ITU Support web site, <http://itusupport.gmu.edu>.
- Windows users should regularly install Microsoft suggested critical updates found at <http://windowsupdate.microsoft.com>.
- When making purchases or filling out online forms with sensitive information, be sure you are making a secure transmission. Signs of a secured transmission will be an URL that begins with <https://> and/or a lock icon on the status bar. 
- Set a password protected screen saver for 10-15 minutes. This protects your data when you walk away from your computer.
- Use Secure Shell for encryption of remote file access and transfers. Available online at <http://itusupport.gmu.edu>. Click on “downloads.”
- Report computer violations to StopIt (abuse@gmu.edu). Please read about what kinds of abuses should be reported at <http://itu.gmu.edu/security/practices/report-abuse>.
- Spam is a nuisance. Read what George Mason can and cannot do about spam: <http://itu.gmu.edu/security/aboutspam.html>.
- Back up important files. Remember to clearly label your disks, zip, or CDs.
- Power off the computer at night to minimize the time bad people can access your files.

S.E.C.U.R.E. I.T. Is EVERYONE'S DUTY.

STEPS TO S.E.C.U.R.E. I.T. ARE:

Simple (All users can implement these procedures)

Effective (Many security problems can be solved by following the procedures)

Concerned (All users should be concerned about security)

Useful (Security procedures keep resources safe and available)

Responsibility (All users must follow the Responsible Use of Computing Policy)

Economical (Resources are protected and staff time is conserved)

Information (Protecting confidentiality, integrity, and accessibility)

Technology (Equipment is protected, hardware is preserved)