Prevention & Protection

IT SERVICES
https://itservices.gmu.edu/

IT SECURITY OFFICE
https://itsecurity.gmu.edu/
Symantec Endpoint Protection Anti-Virus software

https://itservices.gmu.edu/downloads/Antivirus-Information.cfm
FAKE Virus protection

Fake Security Essentials

Potential threat details

Microsoft Security Essentials detected potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action. Click 'Show details' to learn more.

<table>
<thead>
<tr>
<th>Detected Item</th>
<th>Alert level</th>
<th>Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Win32/Trojan</td>
<td>Severe</td>
<td>Remove</td>
<td>Suspended</td>
</tr>
</tbody>
</table>

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommendation:** Remove this software immediately.

Microsoft Security Essentials detected programs that might compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the 'Clean console' action and click 'Apply actions'. If this action is not available, log on as administrator or ask the local administrator for help.

**Items:**

C:\program files\microsoft\security\client\msasec.exe

www.malwarehelp.org
Fake Windows Scanner

Overall System Scan:

<table>
<thead>
<tr>
<th>Components</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Safety</td>
<td>26%</td>
</tr>
<tr>
<td>Network Security</td>
<td>22%</td>
</tr>
<tr>
<td>Private Data Protection</td>
<td>34%</td>
</tr>
<tr>
<td>Hard Disk Optimization</td>
<td>27%</td>
</tr>
<tr>
<td>Media Components</td>
<td>50%</td>
</tr>
<tr>
<td>Memory &amp; Devices</td>
<td>33%</td>
</tr>
</tbody>
</table>

Scan Disks
- Viruses: 16 Kernel misconfigured
- System errors: 36 Privacy data leak
- Registry errors: 165 Slow internet connection

Additional Info:
The analysis of system data protection parameters revealed the low security level of system components. Potentially harmful software that may compromise your system integrity has been detected.
The structure of some files shows code elements that can be considered as malicious. Please make sure all security parameter settings for system components and services are configured correctly as well as the software and system files communication settings.

Microsoft Windows XP
Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz
Fake Anti-Malware
User Education

• Working with Mac users to help them understand that significant threats to Macs do exist. More will arrive as Macs become increasingly popular in business, and social engineering attacks are as likely to victimize Mac users.
Gatekeeper

- OS X 10.8 Mountain Lion, Apple introduced Gatekeeper, which manages code execution permissions for code obtained through approved software.

- Mac version of Java was recently hardened, and Adobe Flash is gradually being replaced by HTML5.
FileVault

• FileVault 2 uses full disk, XTS-AES 128 encryption to help keep your data secure. With FileVault 2 you can encrypt the contents of your entire drive.

• Your password and Recovery Key are critical.

• Please take note that the encryption used in FileVault will make accessing data on your encrypted drive impossible without the permitted user accounts' passwords or the recovery key.
Firewall

• The firewall should be turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.
Password

- Disable Automatic Login
- Require password with screen saver
- Change the password to match your NetID's
Time Machine

- Time Machine automatically backs up your entire Mac.

- Time Machine keeps hourly backups for the past 24 hours, daily backups for the past month, and weekly backups until your backup drive is full.

- The only thing you need to do is plug in an external hard drive.
The website "epatriot.gmu.edu" contains a Java applet. Do you want to allow the applet to load?

You can manage which websites are allowed to load Java applets in Safari Security preferences.

Block  Allow