Information Security Guidelines for International Travel

Travelling to remote sites, and especially international locations, increases information security risk. Specifically:

- Information security is often not taken seriously; and equipment at the site may not have anti-virus, anti-spyware or firewall software. This almost guarantees that malicious software (malware) is present.
- The use of pirated software obtained from questionable sources increases the exposure to malware.
- Less rigorous network security and monitoring allow malware to spread on the site's network without limits.

Faculty travelling to teach at international sites should take the following precautions:

- Beware of behavior that may put your information at risk. For alternatives to common tasks, see the table below.
- Do not connect a USB flash drive from anyone (student or faculty) to your computer. Malware can spread as soon as the drive is inserted.
- Check out an SCOB laptop to use at the remote site. The laptop will have properly configured security software.

> ***When using your personal equipment, IT will not be able to help solve any problems that may arise during your trip.***
>
> ***If an SCOB laptop becomes infected with malicious software, it will be restored to its initial state upon return to campus. No data loss will result from that operation. If your personal laptop needs to be restored, data loss is likely.***

Operation	More Secure Alternative
Using USB flash drives to transfer information between your computer and an institutional computer	• Use a writeable CD on your computer to record the files. Most malware will not be able to replicate itself to your machine because it will not be able to write to the CD. • Use a USB flash drive with a "write protect" switch, which will turn the drive into a read-only device. • Transfer files back to your computer via e-mail. The TROY mail system will check attachments for viruses.

Operation	More Secure Alternative
Logging on to any password-protected site (e.g. TROY e-mail, WebExpress, Blackboard, etc.) from a public computer. **The public computer may be infected with keystroke logging malware, thereby capturing your username and password.**	• Refrain from using a public computer for any purpose (this applies to institutional computer labs, but also hotel "business centers" and Internet cafes).
Connecting to a wireless network: any information transmitted on most wireless networks is easily intercepted.	• Refrain from connecting to wireless networks. Even though wired network data can also be intercepted, it is harder to accomplish than on wireless networks.

Beware of the following signs of infection on computers:

- Excessive popups that start as soon as the computer is booted or the web browser is opened.
- Anti-virus software that cannot be turned on.
- Problems with network connectivity.
- Unresponsiveness at times.

For more information, or to reserve a laptop, please contact:

Sven Aelterman
Web/Technology Specialist
Sorrell College of Business
213 Bibb Graves Hall
Troy Campus

For other campuses and colleges, please contact your local IT representative.