

# Cyber Security Awareness Day



## October 17, 2006 Memorial Union Lecture Bowl

**9:00 am-10:00 am**

*Trusted Platform Module (TPM) and  
Secure Data Sharing*  
Wave Systems

**10:30 am-11:30 am**

*Law Enforcement Trends in  
Cyber Crime*  
FBI Cyber Crimes Task Force

**10:30 am-11:30 am**

(concurrent session in the River Valley Room)  
*Software Security in the Real World*  
Foundstone Professional Service  
(a Division of McAfee)

**12:30 pm-1:30 pm**

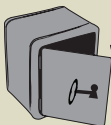
*Identity Theft: When bad things  
happen to your good name*  
US Postal Inspection Service

**2:00 pm-3:00 pm**

*Introduction to Personal Internet  
Safety & Security*  
Foundstone Professional Service  
(a Division of McAfee)

**3:30 pm-4:30 pm**

*Securing the Infrastructure*  
Cisco Systems



# SAFE

Security Awareness  
For Everyone

UNO Cyber Security Awareness Day

# *Six Cyber Security Practices for Safer Computing*

## **1. Protect your personal information.**

Don't share your personal information (especially your Social Security Number, account numbers, or student or employee id number) unless you know who you are dealing with and how it will be used and protected. Don't reply to or click on links in any email asking for your personal information.

## **2. Know who you're dealing with.**

Be suspicious of free software and file sharing – it may come with spyware. Use anti-spyware software such as Windows Defender (<http://www.microsoft.com/defender>) or a web browser plug-in like McAfee's SiteAdvisor (<http://www.siteadvisor.com/>).

## **3. Use anti-virus software and a firewall, and update regularly.**

UND provides McAfee antivirus software for free at <http://itsecurity.und.edu/virus.html>. All students, faculty, and staff at UND can install this software on their work and/or personal computer. Also, you should turn on the built-in firewall on your Windows XP or Mac OSX computer.

## **4. Configure your operating system to update automatically.**

You should make sure to update your Windows, Macintosh, or Linux operating systems regularly with the latest patches. Most operating systems can be configured to update automatically.

## **5. Protect your passwords.**

Keep your passwords in a secure place, and don't share them with anyone. Passwords should be at least eight characters, contain upper and lower case letters, numbers and special characters, and should not be words found in the dictionary.

## **6. Back up important files.**

You should think twice about storing sensitive or personal information on your desktop or laptop computer –consider using a departmental or secure server instead. If you must store important data on your computer, consider encrypting it and back it up by copying it to a removable storage device and storing it in a safe place.