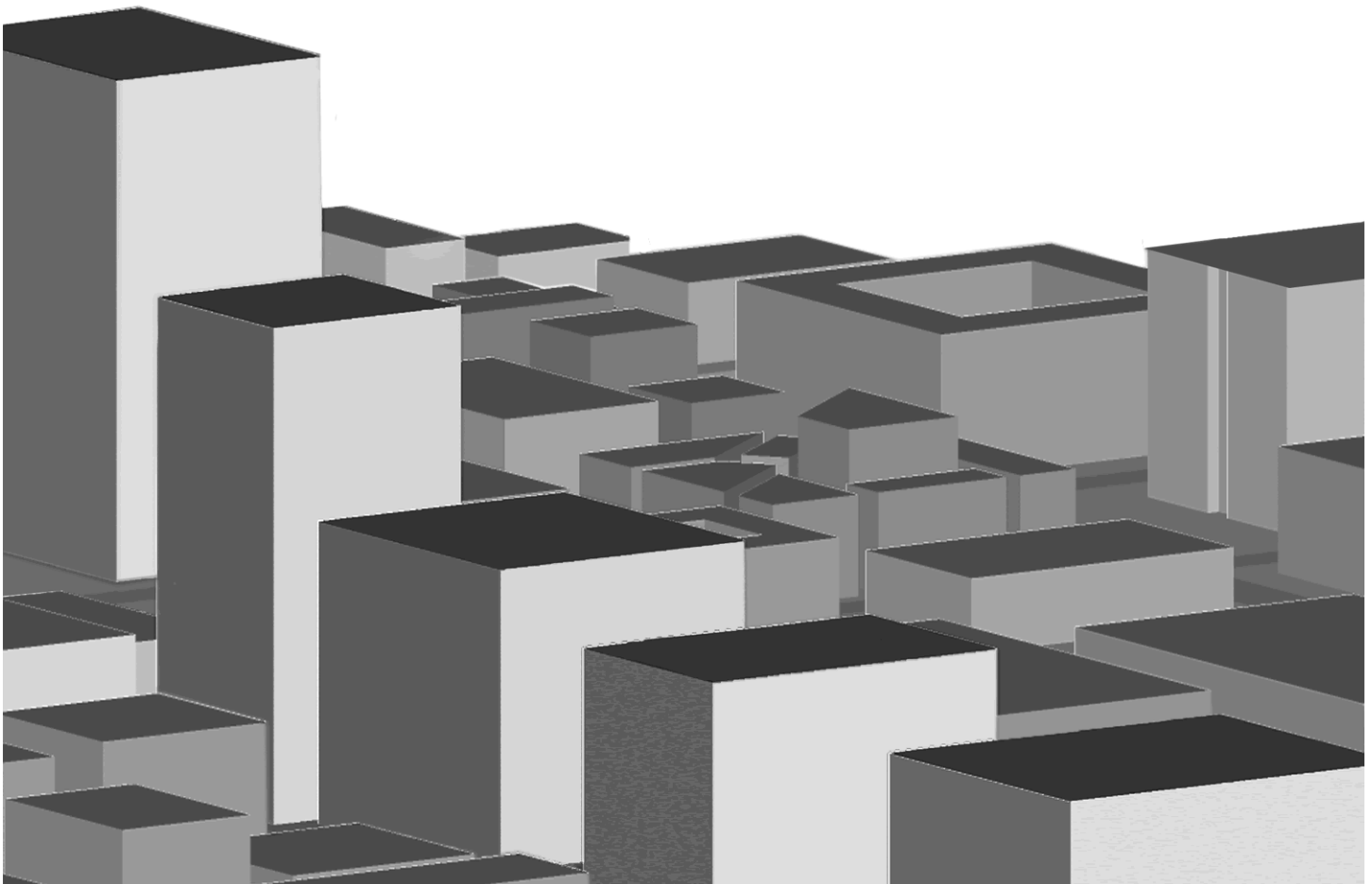




Windows: End-User Security



About IT Training & Education

The University Information Technology Services (UITS) IT Training & Education program at Indiana University offers instructor-led computing workshops and self-study training resources to the Indiana University community and beyond. We deliver training to more than 30,000 participants annually across all Indiana University campuses. Our staff is comprised of enthusiastic professionals who enjoy developing and teaching computing workshops. We appreciate your feedback and use it to improve our workshops and expand our offerings. We have received several national awards for our materials and they are being used at universities across the country. Please keep your questions, comments and suggestions coming!

In Bloomington, contact us at ittraining@indiana.edu or call us at (812) 855-7383.

In Indianapolis, contact us at ittraining@iupui.edu or call us at (317) 274-7383.

For the most up-to-date information about workshops and schedules, visit us at:

<http://ittraining.iu.edu/>

Copyright 2007 - The Trustees of Indiana University

These materials are for personal use only and may not be copied or distributed. If you would like to use our materials for self-study or to teach others, please contact us at: IT Training & Education, 2711 East 10th Street, Bloomington, IN 47408-2671, phone: (812) 855-7383. All rights reserved.

The names of software products referred to in these materials are claimed as trademarks of their respective companies or trademark holders.

Contents

Welcome and Introduction	1	Using Windows Update	40
What You Should Already Know	1	Automatically Enabling Updates	43
What You Will Learn	1	Keeping Windows-Based Applications Current	46
What You Will Need to Use These Materials	1	Running Microsoft Office Update	46
Getting Started	2	Using Security Alert Services	46
Today's Project	3	Understanding the Windows Firewall	46
Important Considerations	3	Configuring the Firewall	47
Who Is Responsible for Security?	3	Protecting Against Viruses, Worms, and Spyware	50
General IT Policies	4	What Is a Virus, Worm, or Trojan Horse?	50
IT Policy Office Role	5	Understanding Computer Viruses	51
IT Security Office Role	5	Do's to Avoid Viruses	52
Understanding Terminology Related to Security	7	Don'ts to Avoid Viruses	53
Protecting a Local Machine	8	Introducing the Norton AntiVirus Program	53
Physical Security	8	Protecting Your Machine Before Installing Norton	54
Logging On and Off	8	Understanding Realtime File Protection.	55
Switching to Classic View	9	Understanding the LiveUpdate Feature	57
Locking a Workstation Without Logging Off	10	Understanding Virus Definitions	59
Manually Locking the Workstation	10	Scheduling Regular LiveUpdates	59
Locking the Computer Through the Screen Saver.	11	How Does Virus Scanning Work?	61
Disabling File and Printer Sharing	13	Performing a Manual Virus Scan	61
Managing User Accounts	15	Scheduling Regular Virus Scans.	63
Different Types of University Accounts	16	What if a Virus Is Found?	65
Understanding the Local Administrator Account	17	Protecting Against Spyware and Unwanted Software	65
Securing the Built-In Administrator Account	17	Tools to Help Detect and Help Remove Unwanted	
The Principle of Least Privilege	18	Software	66
Option 1: Only the LSP Manages the Local Machine	19	Using Email Safely.	67
Option 2: The User Manages the Local Machine	19	Protecting Against Dangerous Attachments	67
Renaming the Built-In Administrator Account	19	Note on Outlook E-Mail Security Update	68
Changing the Password.	21	Protecting Against Spam	68
Removing Your Domain Account from the Local		Strategies for Dealing with Spam	69
Administrators Group.	22	Protecting Against Phishing (Spoofing)	69
Adding Your ADS Domain Account to the Users		Protecting Your Privacy	70
Group	23	How to Know if a Web Site Is Secure	71
Creating a New User Account	26	What Are Cookies?.	71
Performing Administrative Tasks Using the Run As		Viewing Cookies and Changing Preferences	72
Command	29	Using Microsoft Internet Explorer to Control	
Using Passwords Effectively.	31	Cookies	72
Creating Good Passwords	31	Blocking Pop-Ups in Internet Explorer	74
Things to Avoid when Choosing a Password	32	Using Mozilla Firefox to Control Cookies	75
Managing Passwords	32	Blocking Pop-ups in Firefox	76
About Sharing Passwords	33	Deleting the Browser Cache.	77
Changing Passwords Frequently	33	Clearing the Recent Documents List	79
Keeping Windows XP Updated	34	Connecting to a Network Via a VPN.	80
Different Types of Updates	34	Online Resources.	82
Using the Microsoft Baseline Security Analyzer	35	Wrapping Up.	83
Running the MBSA	36	Contributions to These Materials	84

Welcome and Introduction

Welcome to *Windows: End-User Security - What You Don't Know CAN Hurt You*.

What You Should Already Know

You should have already attended *Windows: Basic Computing Skills* or have the equivalent skills. Specifically, you should be able to:

- Use the mouse
- Use standard Windows-based applications
- Switch between applications and documents
- Navigate a Web page

What You Will Learn

This workshop provides information and guidelines on how to keep computers more secure from external threats.

In this workshop, you will learn how to:

- Use common terminology associated with Windows security
- Protect a local machine
- Manage user accounts and passwords
- Keep Windows XP and Windows-based applications updated
- Guard against computer viruses, worms, and spyware
- Use email safely
- Protect your privacy

What You Will Need to Use These Materials

To complete this workshop successfully, you will be provided with:

- The use of a PC running Windows XP Professional Operating System
- The use of a Web browser

Getting Started

These materials assume you will begin work from the desktop.

Logging On

In some instances, you may need to log on to your computer before starting. If you need assistance logging on, please consult your instructor.

Starting an Application

These materials assume that you are able to launch an application. If you need help starting an application, please ask your instructor.

Finding Help

If you have computer related questions not answered in these materials, you can look for the answers in the UITS Knowledge Base, located at:

<http://kb.iu.edu/>

Online Training

Want to learn more? IT Training Online makes self-study IT courses available to the statewide Indiana University campus community. To find out more, go to:

<http://ittraining.iu.edu/online/>

Members of the general public can purchase access to self-study courses through the CLN Continuing Studies program at IUPUI. For more information, go to:

<http://www.cln.iupui.edu/>

Getting the Exercise Files

Most of our workshops use exercise files, listed at the bottom of page 1 of the materials. In our computer-equipped classroom, these files are located in the eclass folder, which is on your desktop. If you are using our materials in a different location, you can obtain the exercise files from our Web site at:

IUB: <http://ittraining.iu.edu/iub/materials/>
IUPUI: <http://ittraining.iu.edu/iupui/materials/>

Once you are logged on and have the needed files or the eclass folder on your desktop, you are ready to proceed with the rest of the workshop.

Today's Project

Every year computers become more vulnerable as new security threats increase. Security is a very important concern for users of the Windows operating system. We, as users, must take responsibility to try to protect our computers from external threats as much as possible. The threats are numerous and constantly increasing.

In today's workshop, we will discuss security issues as well as vulnerabilities and threats that affect anyone running the Windows operating system. We hope to increase security awareness and present guidelines that will be helpful to those interested in protecting their own computer systems. Many links to online resources will be provided throughout the workshop for your future reference.

Important Considerations

During this workshop, you will follow your instructor through a Web site that gives a summary of these materials by clicking on the appropriate buttons. We will be using the current versions of Windows XP and Microsoft Internet Explorer.

Due to limitations on the STC lab computers, most of the exercises will be demonstrated through simulations on the Web site at:

http://ittraining.iu.edu/workshops/win_security/

A padlock icon will appear at the beginning of each section in the materials that has a simulation.

If you are a staff member at Indiana University, then your machine may be managed by a professional local support provider (LSP); therefore, you may not have privileges to make all the changes which are taught in this workshop. However, the information will still be valid because you will better understand what it is that your local support provider actually does for you and why. In addition, the information you learn in this workshop can be applied to your home computers.

Who Is Responsible for Security?

Security is a responsibility shared between the organization that owns the system, the system administrator, anyone who uses the system, and anyone who walks in the room where the system is located. All University faculty, staff, and students are entitled to the privilege of accessing computing resources and

network capacity, as well as those individuals outside the University for purposes consistent with the University's mission. Certain responsibilities accompany that privilege.

The computer user at IU is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security and confidentiality of information stored on it. Examples of the user's responsibilities are as follows:

- To protect computer accounts, passwords, and other types of authorization that are assigned to individual users.
- To always log out of accounts and shared computers.
- To understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.
- To take steps to understand computer viruses and other destructive programs and to take appropriate action to protect your accounts and computers from such threats.
- To honor and maintain all of IU's system security procedures and confidential information.
- To use accounts for legal purposes only and to uphold all software copyrights and license agreements.

For policy statements indicating what the general privileges and responsibilities are within the University computing environment, see the *Computer Users' Privileges and Responsibilities* page at:

<http://www.itpo.iu.edu/policies/cupr.html>

By accepting an IU computing account, you are responsible for following all applicable IU policies, some of which are summarized below.

General IT Policies

University Information Technology Services (UITS), together with computing centers at each campus, as well as many academic departments and administrative units, have responsibility for providing and maintaining shared computing tools. General policies regarding the resources IU provides are outlined as follows:

- Access—Indiana University will provide access to appropriate central and campus computing resources, and to their attached networks, to all members of the University community whose work requires it. Fees are charged for some services.
- Availability—Indiana University will make its central and campus computing resources and networks available to users with the fewest interruptions possible.

Some university units such as colleges and departments may have in place more specific policies related to the use of information technology. For policy statements on university-wide, campus-wide, or departmental IT policies, go to:

<http://www.itpo.iu.edu/policies/>

IT Policy Office Role

The University Information Technology Policy Office (ITPO) provides assistance in reviewing specific situations and analyzing and determining appropriate IT policy. This office also coordinates response to incidents of abuse or inappropriate use of information or information technology, such as security breaches, compromised machines, and copyright infringement.

The policies maintained by this office apply to all units on all eight campuses and provides basic IT policies on such issues as:

- Computer Users' Privileges and Responsibilities (CUPR)—Reflects the general ethical principles of the University community and indicates, in general, what privileges and responsibilities are characteristic of the University computing environment.
- Use—Reflects the policy on what IU technology resources can be used for, which does provide for “incidental personal use.”
- Sanctions—Specifies disciplinary procedures for violation of policies.
- Privacy—Specifies situations when a user's stored computer information can be accessed. Policy basically states that no one can look at your files or email without appropriate justification. There are exceptions as to when your files can be accessed and what the appropriate justification is in those cases.

For more specific information on the IT Policy Office, go to:

<http://www.itpo.iu.edu/>

IT Security Office Role

The University Information Technology Policy Office (ITPO), with the University Information Technology Security Office (ITSO), assists in responding to and investigating incidents related to misuse or abuse of Indiana University information technology resources. This includes computer and network security breaches and unauthorized disclosure or modification of electronic institutional or personal information.

Other services of the ITSO role are to:

- Provide IT security awareness and education
- Provide IT security guidelines and standards
- Provide security consulting and review
- Maintain production services
- Investigate and document IT security incidents

For IT incidents involving threats to personal safety or physical property, immediately contact the campus police department. For electronic information and/or systems security incidents requiring immediate attention, call your local Campus Support Center or send details to the email address:

it-incident@iu.edu

To stay informed of security issues, you may view bulletins or subscribe to receive ITSO bulletins by email at:

<http://itso.iu.edu/ITSO-Bulletins/>

For general information on the IT Security Office and its services, go to:

<http://itso.iu.edu/>

Sample for review use only

Understanding Terminology Related to Security

Listed below are some commonly used terms:

- **Adware**—A general term used for software that invades your computer in the form of persistent pop-up ads.
- **Cracker**—someone who looks for and breaks into computers or networks without authorization, either for the fun of it or to steal valuable information such as credit card numbers; also called a “black hat” hacker.
- **Denial of Service Attack (DoS)**—A term used when an attacker attempts to prevent legitimate users from accessing information or services. The most common and obvious type of DoS attack occurs when an attacker “floods” a network with information.
- **Hacker**—a general term used for anyone who spends time poking into computers and operating systems, trying to discover their vulnerabilities.
- **Intruder**—an unauthorized individual who tries to access a computer system from outside, also referred to as an attacker.
- **Malware**—A new term which is emerging to refer to any software with malicious intent. Term is derived from **malicious software**.
- **Probe**—a program used to gather information about a system or its users.
- **Risk**—the probability that a vulnerability will cause a harmful result.
- **Social Engineering**—the practice of obtaining confidential information by manipulation; for example, people claiming to be administrators may trick computer users in to divulging sensitive information such as passwords.
- **Spyware**—a general term used for software that performs certain “secret” behaviors such as advertising or collecting personal information, generally without obtaining your consent.
- **System Compromise**—a violation of security policy in which disclosure of sensitive information may have occurred.
- **Threat**—any event with potential to harm a system by means of destruction, disclosure, modification of data, and/or denial of service.
- **Trojan horse**—“back door” software programs that allow intruders to take remote control of a computer without the owner’s knowledge. Trojans can be installed on computers through thousands of free software packages that can be downloaded from the Internet.
- **Virus**—a piece of code that replicates by attaching itself to another object. It can attack the registry, replace system files, or take over email programs in its attempt to replicate itself.
- **Vulnerability**—a weakness in system security procedures that may be used to violate a system security policy.
- **Worm**—an independent program that replicates by copying itself from one computer to another, usually over a network or through email attachments. A particularly common use of worms is to make computers spew out so much bad network traffic that they cause networks and servers to fail.

Protecting a Local Machine

It may seem that credit card theft and outbreaks of email viruses are the only serious threats that affect our computer systems. However, attacks can come from just about anywhere, including your own office. An attacker who gets physical access to your local computer for just a few minutes can plant dangerous software programs on your computer and literally take remote control without your even knowing it. In the past, an attack may have cost you your data, or necessitated an expensive computer repair. Now an attack can cost you your identity and money, and can destroy your credit history.

Listed below are the most important tasks that are covered in this section:

- Make sure that your computer is physically secure.
- Lock your workstation when away from your desk.
- Secure the local administrator account.
- Use a non-administrative account for everyday use.
- Disable File and Print Sharing.

We will look at several ways to begin securing a local machine.

Physical Security

Physical security is the first step in protecting a local machine. The attacker does not have to have any technical skill at all if a notebook computer is left unattended for even a few minutes. As a comprehensive computer security plan, the absolute first line of defense is to make sure that your computer is physically protected.

Some guidelines to make sure your computer system is protected include:




- Keeping any computer containing sensitive information behind a locked door.
- Taking extra precautions to protect hand-held devices and notebook computers. You may consider using a radio-controlled alarm, which sounds an alert if you and your notebook carrying case are unexpectedly separated.
- Using external locks to physically bolt computers to desks or hooking computers to a security system.
- Watching out for “shoulder surfers” who try to steal passwords by watching your fingers type as you log on.

Logging On and Off

Windows XP Professional is generally used in a networked environment, but you do not have to be connected to a network domain to run it. You might have Windows XP Professional installed on a laptop computer that you use both at the office and at home. When you log on to a computer that has been,

but is no longer, connected to a network domain, you log on in the ordinary manner. Your information is validated against information that was stored on the computer the last time you logged on to the domain.

Windows XP Home Edition is designed for home computers that are not operating within a network domain. This workshop will focus on Windows XP Professional installed on a network domain and will depict screenshots from the Windows XP Professional user interface.

Pressing  +  +  (known as the *secure attention sequence*), to log on or off ensures that your password remains secure because it prevents programs called Trojan horses, which might have been planted on your system by hackers, from capturing your user account name and password. A user with administrative privileges can change this requirement so that this secure attention sequence is not required, but making this change is definitely not recommended.

1. To begin logging on to a computer, press:



NOTE: To require or disable this secure attention sequence, go to the Control Panel, open User Accounts,  the Advanced tab, select the Require Users to press  +  +  checkbox.

2. To log on to a computer, at the log-on screen, type:

your User name and Password

3. To continue,



Switching to Classic View

The new Windows XP interface looks somewhat different from the previous interface; however, you may be accustomed to the previous and more familiar menu style, which is called the *Classic* Start menu style. For purposes of this workshop, we will use the Classic Start menu interface.

1. To revert to the Classic Start menu style, on the Taskbar, if necessary,



 the radio button for Classic Start menu

In this workshop, we also be using the Classic view for the Control Panel.

2. Open the Control Panel.
3. To switch to Classic view, in the left pane of the Control Panel, if necessary,



4. Close the Control Panel.

Now both the menu interface and the Control Panel will be displayed in Classic view.

Locking a Workstation Without Logging Off

Each time you leave your computer, either at your desk or in a computer lab, the computer is vulnerable. Therefore, it is always a good idea to log out or lock your computer before leaving it, even if you plan to be away for just a few minutes. When locking your computer, any open applications, files, and folders remain open, but you can only continue working after entering your user password.

NOTE: A recommended practice at Indiana University is to log out rather than locking your workstation for long periods of time such as overnight or weekends.

We will explore locking a workstation by using the keyboard command and also by password protecting the screen saver.

Manually Locking the Workstation

Follow these steps to lock your workstation by using the keyboard command.


1. To begin to lock the computer, on the keyboard, press:



The **Windows Security** dialog box appears.

2. To lock the computer,

 Lock Computer

NOTE: An alternative to locking your computer is to press the  and the L key on the keyboard.

3. To begin to unlock the computer, on the keyboard, press:

4. To unlock the computer, in the Password field, type:

your user password 

The computer is unlocked. Next, we will lock the computer by password protecting the screen saver.



Locking the Computer Through the Screen Saver

Using a password-protected screen saver is another way to protect your computer from prying eyes when you are away from your desk.

Follow these steps to enable a screen saver with a password.

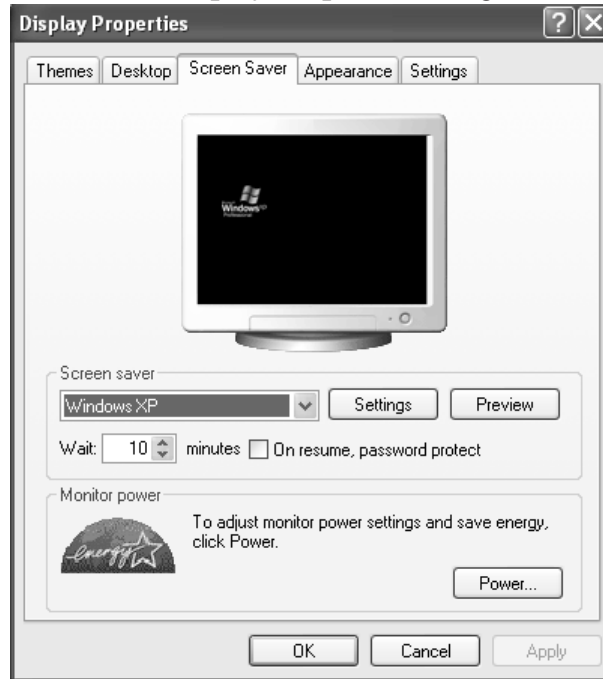
1. To access the Properties dialog box from the desktop,

 the desktop,  Properties

2. To enable the Screen Saver tab,

Click the Screen Saver tab

You see the **Display Properties** dialog box:



3. To select a screen saver file, in the Screen saver drop-down box,

Click , **Click** any screen saver

4. To select the time to wait for screen saver activity, in the Wait field,




set the desired amount of time

This is the number of minutes that will elapse after the last mouse or keyboard activity before the screen saver appears.

- To password protect the screen saver,

 the “On resume, password protect” checkbox,



From now on, when the screen saver comes on, your workstation will be locked until you re-enter your password. The Unlock Computer Window will appear when you press the combination of   . Then you will enter the password for the user name under which you are logged in.



Disabling File and Printer Sharing

Another good practice is to always disable *File and Printer Sharing* on your local machine. This provides added protection against anyone trying to access files on your local machine. The only time that you might want to leave this feature enabled is when you want to allow other users to share resources on your computer, such as files or printers.

NOTE: Check with your LSP before enabling or disabling File and Printer Sharing. Some LSPs may want File and Printer Sharing enabled in order to update departmental machines, and so on.

Follow these steps to disable File and Printer Sharing.

- To begin to disable File and Printer Sharing, on the taskbar,

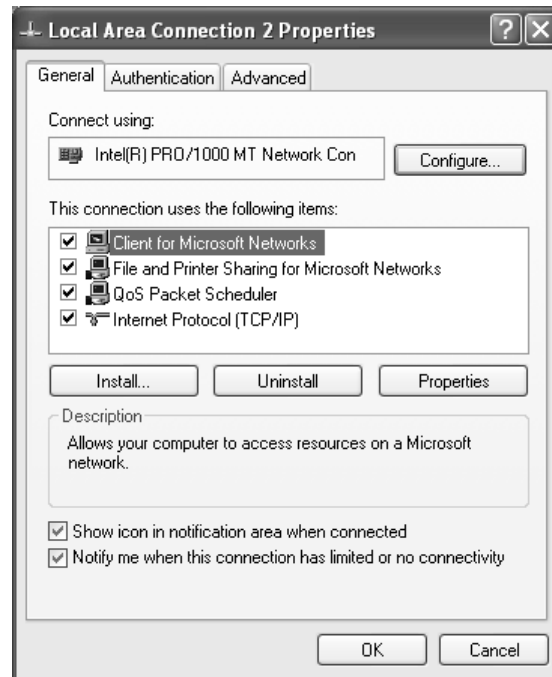
 Start,  Settings,  Control Panel,

 Network Connections

2. To access the Local Area Connection dialog box,

 the Local Area Connection icon,  Properties

You may see a dialog box something like this:



3. Depending upon the current setting, to enable or disable File and Printer Sharing,

 the checkbox for File and Printer Sharing for Microsoft Networks,  

4. Close the Network Connections window.

NOTE: In rare exceptions when you may need to share a resource with others, you should format your drive using NTFS and correctly set the file and directory permissions, which is beyond the scope of this workshop. Also, with Windows 2000 and Windows XP operating systems, new folders are created by default with access granted to the “everyone” group. If you do have file sharing enabled on your computer, be careful to set permissions correctly when creating new folders so that you don’t inadvertently leave them open to everyone on the network.

Managing User Accounts

An **account** is a set of credentials consisting of both a user name and password that allows access to a system's resources. Your computer accounts and passwords are assigned to you alone. You must never share them with others! Protect your accounts by logging out when you are finished using them.

At IU a user name is automatically assigned and consists of letters based on last name, first name, and possibly a middle name. An email address consists of a user name followed by the appropriate campus designation.

When a user creates or gets a new user account and logs on for the first time, a **user profile** is created for that user, which includes the user's environment and preference settings, a set of empty folders, installed applications, desktop icons, and color options. Each user account belongs to a group with permissions to perform certain operations on the computer. The most common groups are:

Group	Permissions
Administrators	Have unrestricted access to the computer.
Power Users	Have most administrative capabilities but with some restrictions; these users cannot modify the Administrators or Backup Operators groups nor take ownership of files.
Users	Are restricted from making system-wide changes.
Guests	Guest accounts are set up for temporary or occasional use and are restricted from making system-wide changes.
Backup Operators	Can override security restrictions for the purpose of backing up or restoring files.

NOTE: Users with Windows XP Home Edition or Windows XP Professional in a standalone environment will see only two levels of user privileges: administrator and limited. Users with computer administrative accounts have permission to do everything. Users with limited access have permissions to do only those things that affect their own account.

Different Types of University Accounts

As a new IU employee or student, you typically receive a Network ID (user name and password) and an ADS domain account as your first computing accounts, which allows you to access a variety of Windows-based services at IU. When you accept computing accounts at Indiana University, you agree to use the University's computing resources responsibly. A major part of responsible use is maintaining the security and confidentiality of your computer accounts and the information you store on them. You are also responsible for following all applicable IU policies.

A **Kerberos** identity is established through a Network ID for authentication on a network. It protects your password by not allowing it to be sent over the network in plain text. To authenticate against the IU.EDU Kerberos realm from a computer running the Windows operating system, the computer must be part of the IU **Active Directory Services** (ADS) or the ads.iu.edu domain at Indiana University. The Active Directory is a hierarchical collection of network resources that can contain users, computers, and printers, which allows administrators to handle and maintain all network resources from a single location. An ADS domain account allows users to gain access to a variety of University network resources. The Network ID account is the user's electronic identity at IU and also gives users authorization to perform such tasks as creating additional accounts, sending and receiving email, or obtaining software via IUware Online.

In summary, an IU student, faculty, or staff member will need a Network ID or ADS domain account in order to:

- Create additional accounts
- Synchronize or change your passwords
- Access your email account(s) on the IU campus
- Access the IU dial-in modems
- Log into any Mac OS X or Windows computer in the IU Student Technology Centers
- Obtain certain software and downloads via IUware Online
- Connect to the IU network via a VPN

To see the various services that can be accessed by both the Network ID and the ADS Domain accounts, go to:

<http://kb.iu.edu/data/ajoc.html>

There are also other types of university accounts used for email, file storage, web space, printing, instructional databases, guest accounts, etc. For more information, click on Accounts and Passwords at:

<http://uits.iu.edu/>

Also, to create new accounts or to manage existing accounts and passwords, you can go to:

<https://itaccounts.iu.edu/>

Understanding the Local Administrator Account

Another type of account is a local Administrator account. A local account is like a domain account except that a local account only controls access to one single, physical computer. Your local account credentials, which include a user name and password, are stored locally on the computer's hard drive, and the computer checks its own files to authenticate your login. This is different from network domain accounts, which are created and stored on domain controllers. The local account's settings determine your rights for running programs, installing and removing programs, accessing files, and enabling or disabling services. Without administrative rights, you cannot perform many system modifications, such as installing software or modifying network settings. The local administrator account cannot access network resources since the local account is recognized only on the local computer; however, it is the account to use when you want to install software or modify system settings.

When you install the Windows XP operating system, a built-in Administrator account is created with full administrative privileges, and each user account you create during setup becomes a member of the Administrators group. This provides convenience because administrative privileges are necessary in order to run many programs. However, always running as a computer administrator makes your computer and network more vulnerable to virus attacks. If a malicious attacker takes control of your machine while you are logged in as an administrator, then he or she will have administrative rights on your local machine. Therefore, for security reasons, one of the first things you should do after installing Windows XP is to rename this built-in Administrator account and to assign it a strong password. Later in the workshop, we will discuss some guidelines for selecting strong passwords.

Securing the Built-In Administrator Account

As mentioned previously, someone who can gain access to your account as Administrator can do just about anything he or she wants with your computer. Since the local Administrator account is a natural target for malicious attackers, it is important that you change the name of the built-in Administrator account and create a strong password for this account if it was not created during the initial install. This makes it more difficult for individuals to use standard dictionary attacks in order to gain access to your local machine. It is also a good practice to remove the default description of this account to help deter attackers.

The procedure for securing the built-in administrator account is:

- Look at the members of the Administrators group to see what accounts are there and why.
- Rename the built-in Administrator account to something other than Administrator.
- Give the built-in Administrator account a strong password if this was not done during the initial setup.
- Remove administrative privileges from accounts that don't need them.

The Principle of Least Privilege

If you look at major threats to computers, they are from user interaction with the Web through tools like browsers and email clients. If you are logged on with administrative privileges and are attacked, a Trojan horse could do things like reformat your hard drive, delete all your files, create a new user account with administrative access, etc. Some malware works only because the user browsing the Web is an administrator. When logged on with administrative privileges, there is much less protection against modifications being made by intruders to system setup and configurations on your local system. Therefore, anyone running the Windows operating system should avoid logging on for everyday use with an account that belongs to the Administrator's group.

The *Principle of Least Privilege* means that the user logs on with an account that has fewer system privileges for everyday or routine activities, such as running Microsoft Internet Explorer or Outlook and instant messaging. Unfortunately, almost all Windows users today continue to use the administrator account for these daily tasks.

Always secure your own system by setting all daily use accounts to run with least privileges. The key is to log in as Administrator only when you need to install software or perform various other administrative tasks. This practice helps to minimize the risk of someone maliciously damaging a system's configuration or infecting the machine with a virus or Trojan horse.

Not only do many Windows users run with an administrator account because "Administrator" is the default new account for Windows XP, but restricting users to a limited account can be frustrating at times because some applications, as well as some Windows-based tasks, expect users to have administrative privileges. As a result, some applications and tasks will fail to operate correctly when launched by a least-privileged user account (LUA). However, developers are constantly trying to improve their programs so that almost everyone can run as an LUA and still complete their regular daily work without encountering undue inconvenience or special workarounds.

In the next section, you will learn how to secure the Administrator account and how to create a new LUA account, depending upon your IU role and the control that you may have over your own local machine.

Option 1: Only the LSP Manages the Local Machine

DO NOT make any changes to any administrative accounts at IU unless you have first checked with your LSP. There must be at least one account that you or someone else can use to gain access to your local computer with administrative privileges. Your LSP may have already set up an Administrator account on your local machine and may not want you to create any new accounts, especially accounts with administrative privileges.

Option 2: The User Manages the Local Machine

If you manage and have control over your own machine, either at work or at home, then securing the built-in Administrator account, as well as creating new accounts, will most likely be your responsibility.

First, we will see how to rename the built-in Administrator account.



Renaming the Built-In Administrator Account

The following steps can be used to rename any user account, but we will rename the built-in Administrator account.

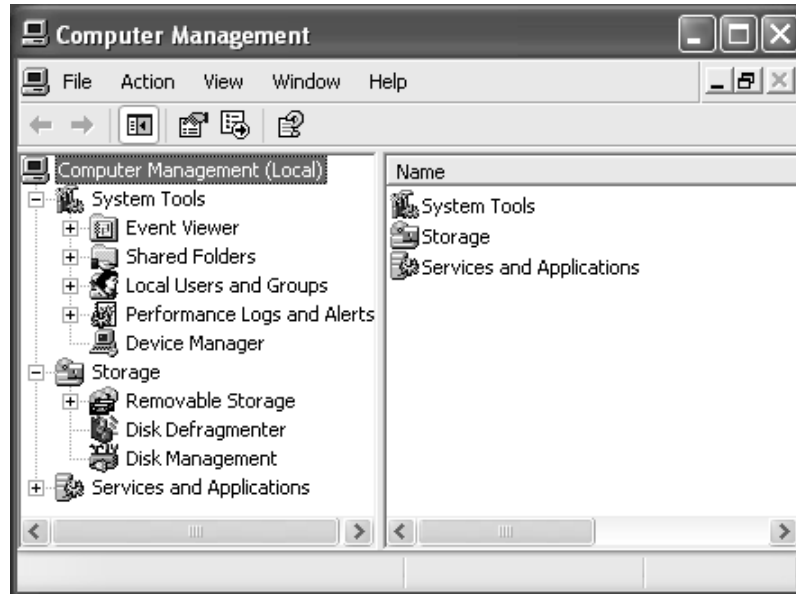
To rename the built-in Administrator account, follow these steps:

1. Log in as the Administrator.

- To open the Computer Management window, on the Desktop,

 the My Computer icon,  Manage

You see the **Computer Management** window:



- Expand Local Users and Groups.
- To expand the Users folder, in the left pane,

 Users

You can see that there is a built-in Administrator account. Any user accounts listed here exist ONLY on the local machine, and the ADS domain (or any other network domain) does not know that they exist.

- To begin to rename the built-in Administrator account,

 Administrator,  rename

A user name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters except the following: “/ \ [] ; | = , + * ? < > . A good “rule of thumb” to use when renaming the administrator account is to use a letter prefix (for example, “A” for administrator) along with the manufacturer service tag number, IU asset tag number, or a home street address number.

NOTE: A renamed user account will retain all of its other properties, such as its description, password, group memberships, etc.

- To rename the built-in Administrator account, type:

the new name 

NOTE: Another default account set up during the Windows XP install is the Guest account, which provides convenient access for occasional users. By default, the Guest account is disabled, but renaming this account may offer a little more protection from would-be attackers, especially if this account is temporarily enabled. If you occasionally need this account, enable it only when necessary. You can rename the Guest account following the same procedure as renaming the Administrator account.

- Close the Computer Management window.

Changing the Password

Another important step in securing the Administrator account is to create a strong password. Next, you will see how to set a new password for the built-in Administrator account, if this was not done during the initial setup.

- Be sure that you are logged in as the Administrator.
- To set a password for the built-in Administrator account, press

  ,  Change password...

For more information on creating strong passwords, see “Creating Good Passwords” on page 31.

- To set a new password, in the New Password and Confirm Password fields, type:

the new password,  

If you want to change the password, enter the old password in the Old Password field. The next time you log off and back on, you will be required to enter the new administrator name and password.

NOTE: You can also change a local user’s password by opening User Accounts in the Control Panel and selecting the user account and choosing Reset Password, but this works only for a local account other than the one with which you’re currently logged on.

- To return to the desktop,



Removing Your Domain Account from the Local Administrators Group

Once you have secured your built-in Administrator account, the next step is to make sure that your everyday user account is not a member of the Administrators group. At Indiana University, the IT Security Office (ITSO) recommends that you normally run your Windows computer as a member of the Users Group and not as an administrator or as a member of the Power Users Group.

Setting up an account with restricted privileges is fairly simple. If the account you use for everyday tasks is your ADS domain account and if it has local administrative privileges, you should change it to a non-administrative account by removing the account from the Administrators group and placing it in the Users group.

If your ADS domain account is a member of the local administrators group, you will need to perform the following steps to remove your domain account from the Administrators group:

- Log in as the Administrator.
- To open the Computer Management window, on the Desktop,



the My Computer icon,  Manage

You see the Computer Management window.

- Expand Local Users and Groups.
- To expand the Groups folder, in the left pane,



- To begin to remove the domain account from the local Administrators group,



You see the Administrators Properties dialog box.

Where to Go From Here

The rest of this document has been intentionally deleted.

To find out how you may use the full version of this document and many other of our award-winning materials in your own training classroom, visit:

<http://ittraining.iu.edu/ematerials/>

