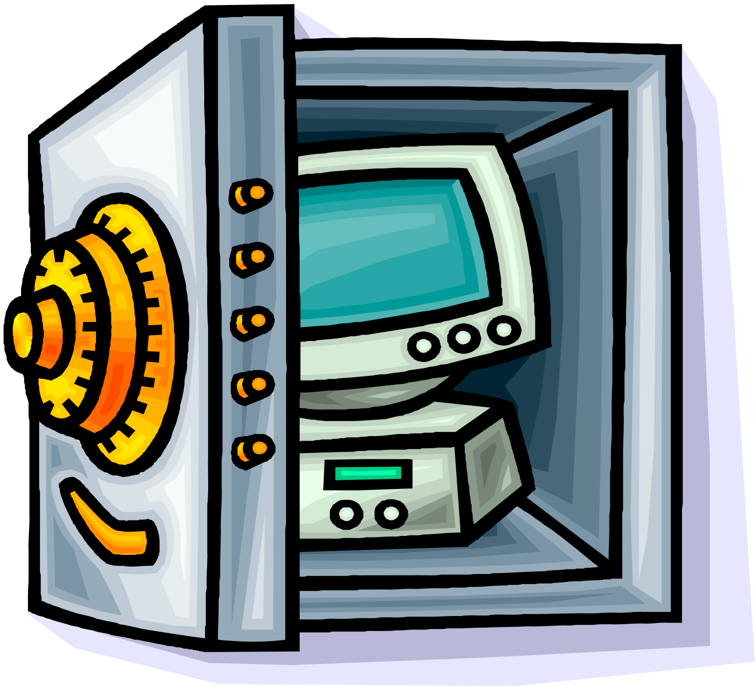
Privacy Preserving Practices and Tools



April 12, 2006

Melissa Dark
Ninghui Li
Clewin McPherson
Joanne Troutner

PURDUE UNIVERSITY
CERIAS

Table of Contents

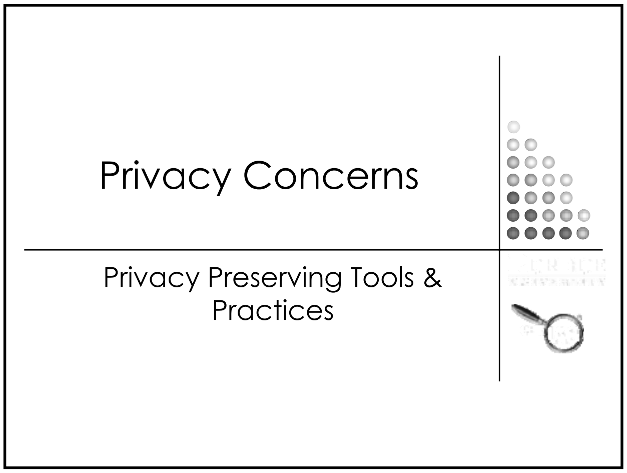
Presenter Backgrounds

Dr. Melissa J. Dark is the Assistant Director for Educational Programs at the Center for Education and Research in Information Assurance and Security. She has extensive experience in science, technology, engineering and mathematics (STEM) education. She has led regional and national faculty and curriculum development projects that improve the capacity of our educational infrastructure to provide educational programs in new and emerging areas, such as Information Assurance. She is leading an initiative to develop the common body of knowledge in Information Assurance, which is not yet a discipline. Dr. Dark is also leading a faculty development project that will train 75 faculty in information assurance so that they can start IA programs at their home institutions. She also oversees the development of multimedia information security training products designed for business and industry.

Dr. Ninghui Li is Assistant Professor of Computer Science at Purdue University. He joined Purdue University in August 2003, after spending three years at Stanford University's Computer Science Department as a research associate. Dr. Li received a Ph.D. in Computer Science from New York University in September 2000. His research interests are in computer security and applied cryptography, including security and privacy in distributed systems, networks, databases, and electronic commerce, with a focus on access control. Ninghui Li has published over 30 papers and has served on the program committees of more than two dozen international conferences and workshops in information security. In 2005, he received the prestigious NSF CAREER award for proposed work on "Access Control Policy Verification Through Security Analysis And Insider Threat Assessment".

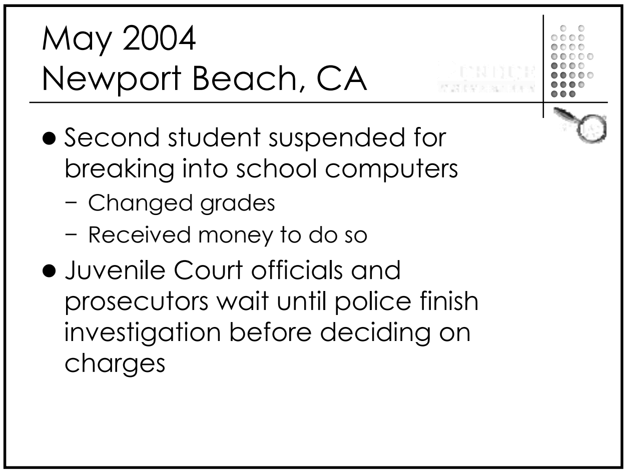
Clewin McPherson is a graduate student in the College of Technology and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. He also obtained his Bachelor's of Science in Computer Engineering from Purdue University. Clewin's research interests include issues of privacy, security and their application in industry.

Joanne Troutner is an experienced classroom teacher and district administrator. She has been a library media specialist for grades K - 12, a 7th and 8th grade English teacher, a consultant for IBM, and is currently the Director of Media/Technology for Tippecanoe School Corporation. Joanne writes a regular Internet Resource column for an international magazine, *Teacher Librarian*. She is the author of *The Media Specialist, The Microcomputer, and The Curriculum*, a pioneering work in the area of technology. Joanne gives technology presentations at local, state, regional, and national conferences as well as for the Bureau of Education and Research (BER). She has also served on the United States Department of Education Telecommunications Task Force and as a grant reviewer for the US Department of Education. Joanne has a BS and MA from Purdue University.



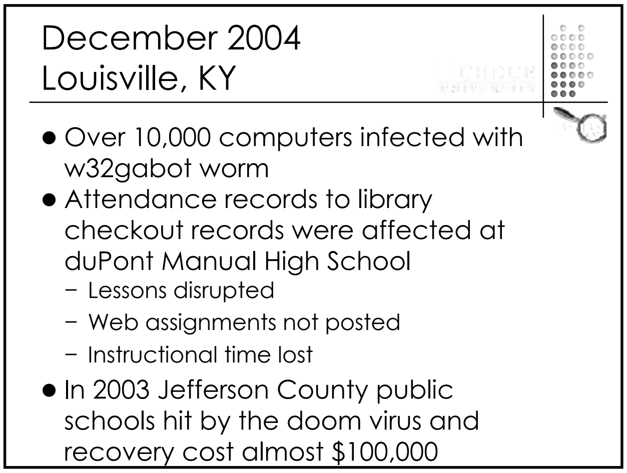
Privacy Concerns

Privacy Preserving Tools & Practices



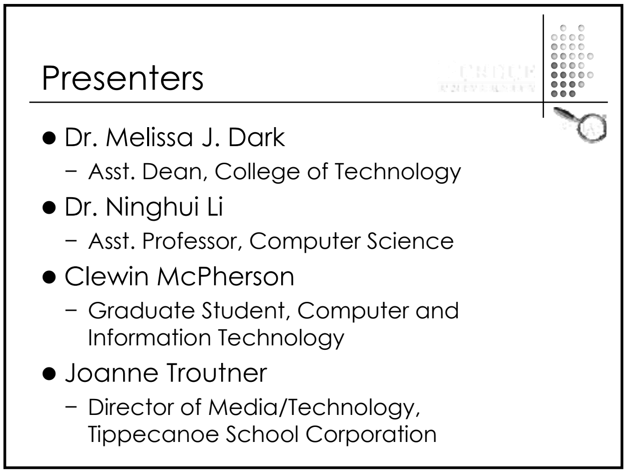
May 2004 Newport Beach, CA

- Second student suspended for breaking into school computers
  - Changed grades
  - Received money to do so
- Juvenile Court officials and prosecutors wait until police finish investigation before deciding on charges



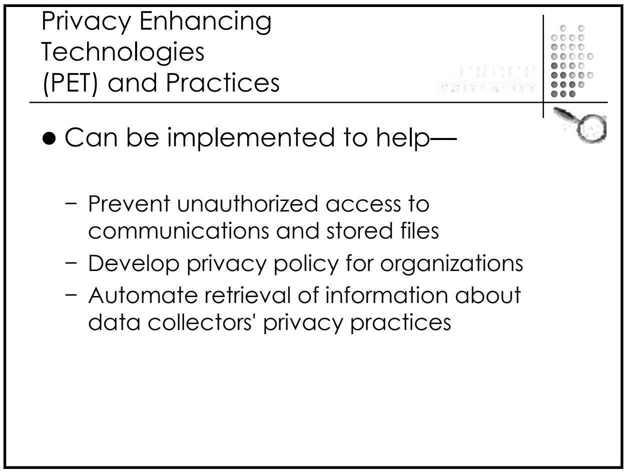
December 2004 Louisville, KY

- Over 10,000 computers infected with w32gabot worm
- Attendance records to library checkout records were affected at duPont Manual High School
  - Lessons disrupted
  - Web assignments not posted
  - Instructional time lost
- In 2003 Jefferson County public schools hit by the doom virus and recovery cost almost $100,000



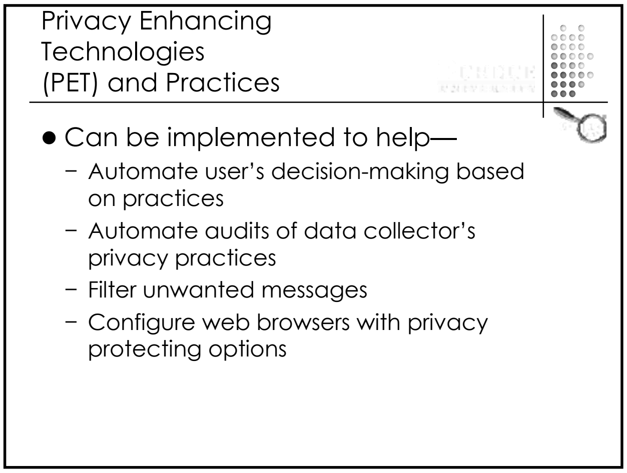
Presenters

- Dr. Melissa J. Dark
  - Asst. Dean, College of Technology
- Dr. Ninghui Li
  - Asst. Professor, Computer Science
- Clewin McPherson
  - Graduate Student, Computer and Information Technology
- Joanne Troutner
  - Director of Media/Technology, Tippecanoe School Corporation



Privacy Enhancing Technologies (PET) and Practices

- Can be implemented to help—
  - Prevent unauthorized access to communications and stored files
  - Develop privacy policy for organizations
  - Automate retrieval of information about data collectors' privacy practices



Privacy Enhancing Technologies (PET) and Practices

- Can be implemented to help—
  - Automate user's decision-making based on practices
  - Automate audits of data collector's privacy practices
  - Filter unwanted messages
  - Configure web browsers with privacy protecting options

Privacy Enhancing Technologies (PET) and Practices

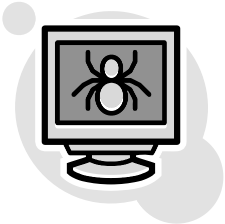
- Prevent automated data capture via cookies, HTTP headers, web bugs, spyware, etc.
- Prevent communications from being linked to specific individual
- Facilitate transactions revealing minimal personal information

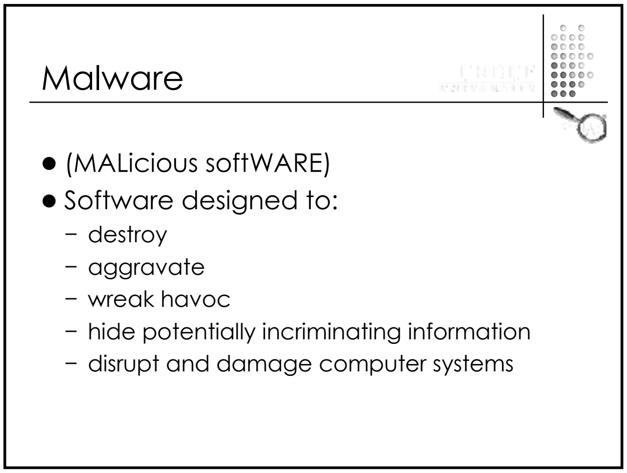
Overview

- Learn about malware and impact on privacy
- Removing malware
- Implementing security tools for privacy purposes
  - For yourself
  - For your district

Learn About—

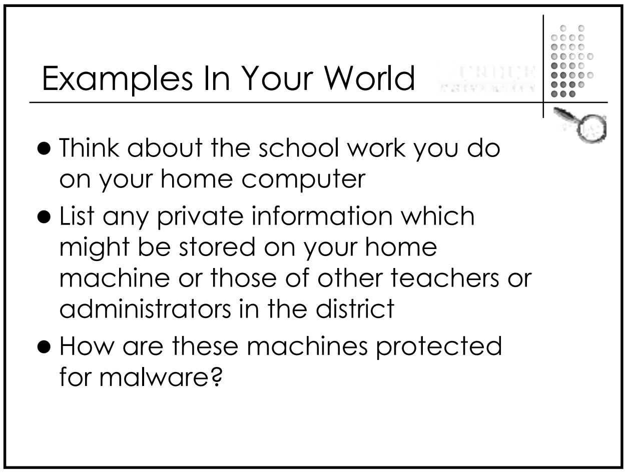
- Privacy Impact of Malware
- Removing Malware





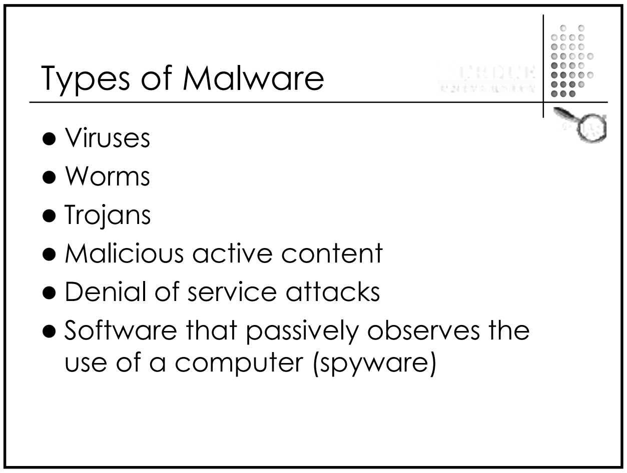
Malware

- (MALicious softWARE)
- Software designed to:
  - destroy
  - aggravate
  - wreak havoc
  - hide potentially incriminating information
  - disrupt and damage computer systems



Examples In Your World

- Think about the school work you do on your home computer
- List any private information which might be stored on your home machine or those of other teachers or administrators in the district
- How are these machines protected for malware?



Types of Malware

- Viruses
- Worms
- Trojans
- Malicious active content
- Denial of service attacks
- Software that passively observes the use of a computer (spyware)

Perfect Malware Removal Tool

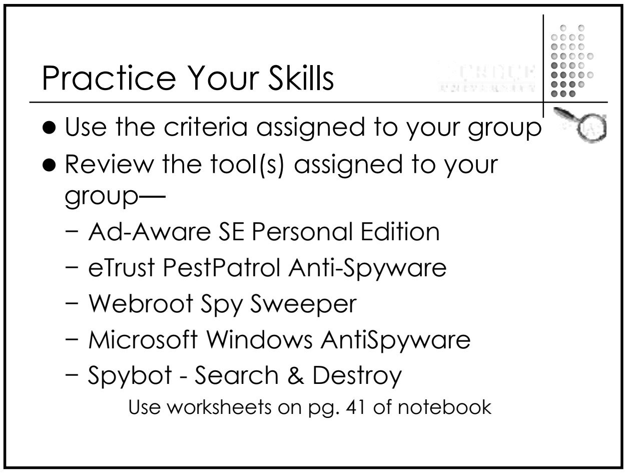
- Work with your group members
- Generate a list of characteristics you want in a “perfect” malware removal tool
- Be prepared to share your list
  - Use worksheet on pg. 40 of notebook

Malware Removal Tools

- Selection Criteria Part 1
  - Reviews / Authoritative tests
  - Constant monitoring / protecting of system
  - Runs at startup
  - Scans processes currently in execution
  - Scans the window registry

Malware Removal Tools

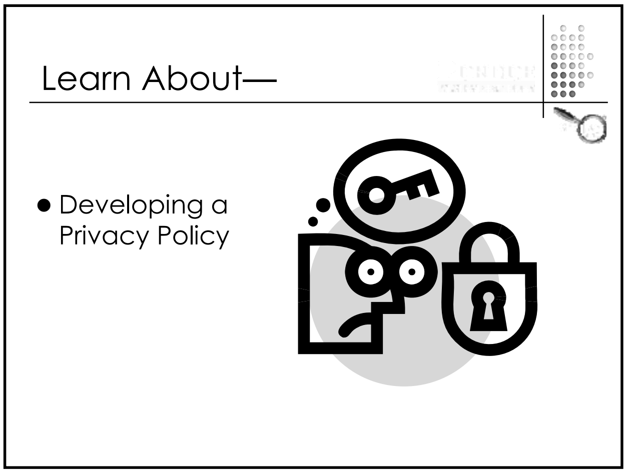
- Selection Criteria Part 2
  - Logs scan results
  - Auto update available / source of monitoring from cve.org, secunia.com, bugtraq or other authority
  - Ability to schedule scans
  - Configurability
  - Ease of Use



Practice Your Skills

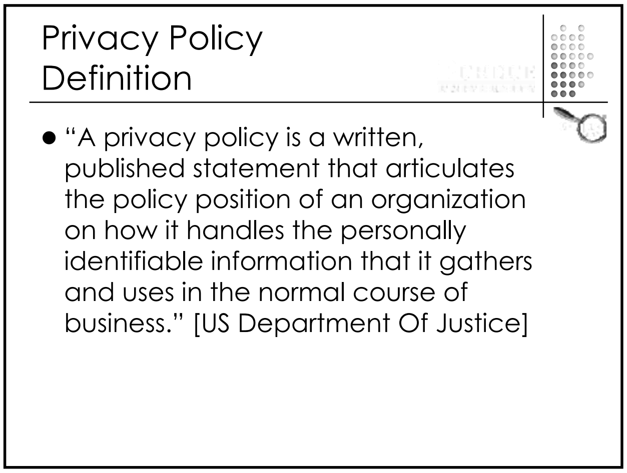
- Use the criteria assigned to your group
- Review the tool(s) assigned to your group—
  - Ad-Aware SE Personal Edition
  - eTrust PestPatrol Anti-Spyware
  - Webroot Spy Sweeper
  - Microsoft Windows AntiSpyware
  - Spybot - Search & Destroy

Use worksheets on pg. 41 of notebook



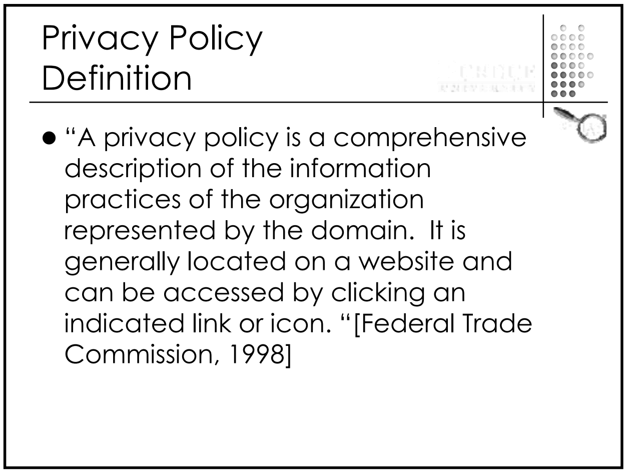
Learn About—

- Developing a Privacy Policy



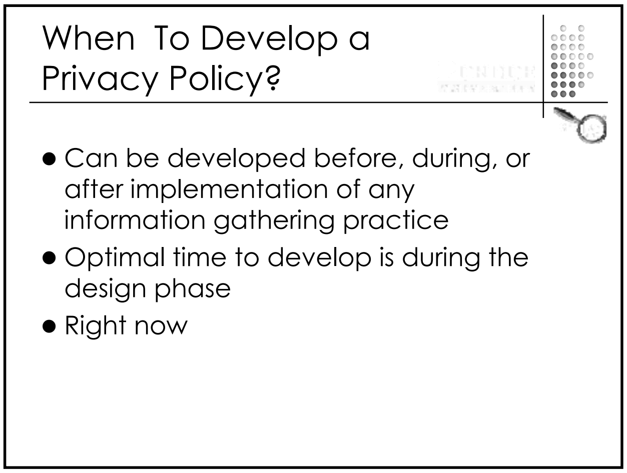
Privacy Policy Definition

- "A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business." [US Department Of Justice]



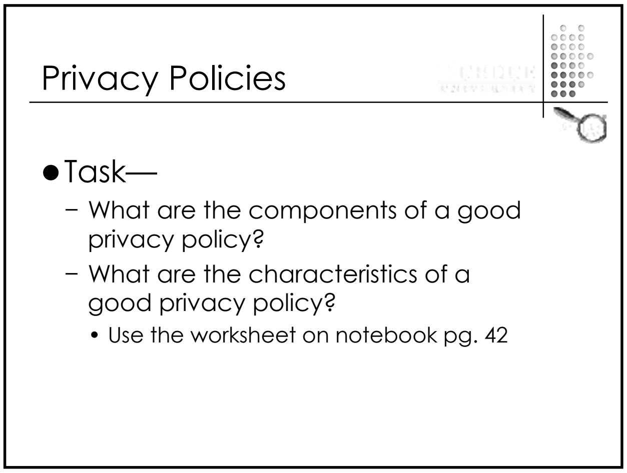
Privacy Policy Definition

- "A privacy policy is a comprehensive description of the information practices of the organization represented by the domain. It is generally located on a website and can be accessed by clicking an indicated link or icon. "[Federal Trade Commission, 1998]



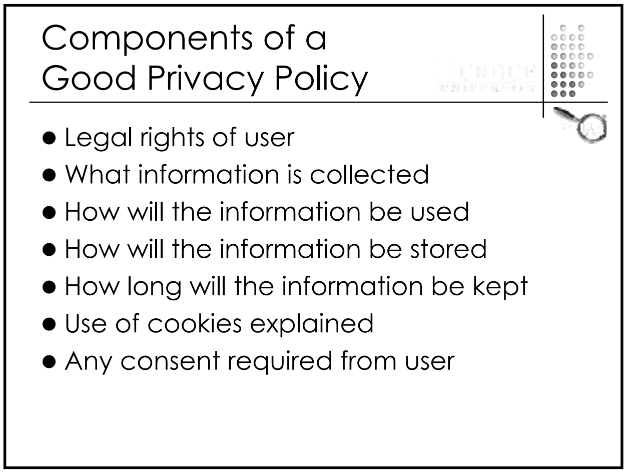
When To Develop a Privacy Policy?

- Can be developed before, during, or after implementation of any information gathering practice
- Optimal time to develop is during the design phase
- Right now



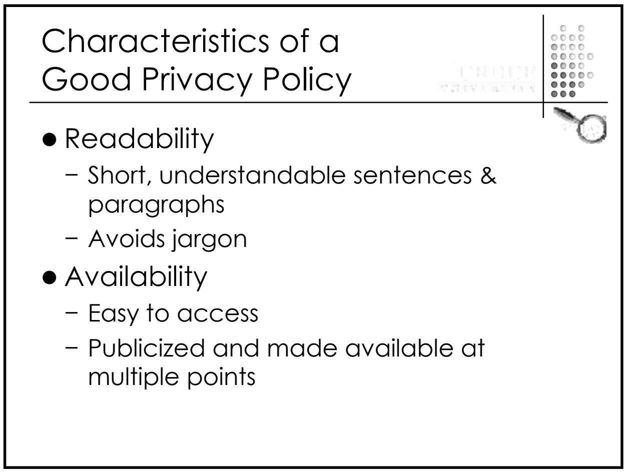
Privacy Policies

- Task—
  - What are the components of a good privacy policy?
  - What are the characteristics of a good privacy policy?
    - Use the worksheet on notebook pg. 42



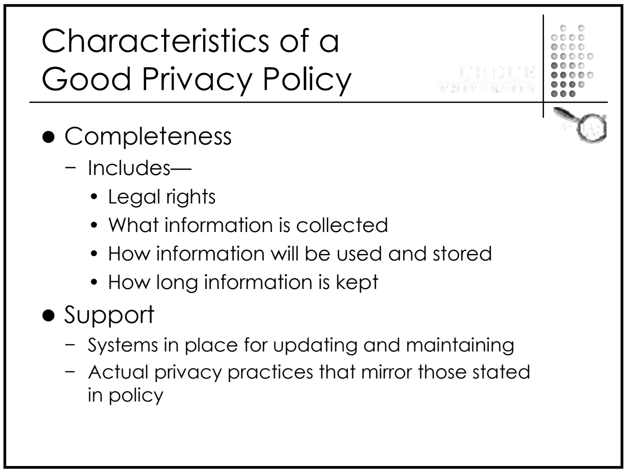
Components of a Good Privacy Policy

- Legal rights of user
- What information is collected
- How will the information be used
- How will the information be stored
- How long will the information be kept
- Use of cookies explained
- Any consent required from user



Characteristics of a Good Privacy Policy

- Readability
  - Short, understandable sentences & paragraphs
  - Avoids jargon
- Availability
  - Easy to access
  - Publicized and made available at multiple points



Characteristics of a Good Privacy Policy

- Completeness
  - Includes—
    - Legal rights
    - What information is collected
    - How information will be used and stored
    - How long information is kept
- Support
  - Systems in place for updating and maintaining
  - Actual privacy practices that mirror those stated in policy

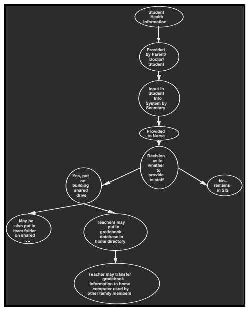
Think About Your World

- Task—
  - What personally identifiable information is collected?
  - *Which is information collected?*
  - *How is information kept or stored?*
  - Who uses information?
  - Who has access to information?
    - Use chart on pg. 43 of notebook

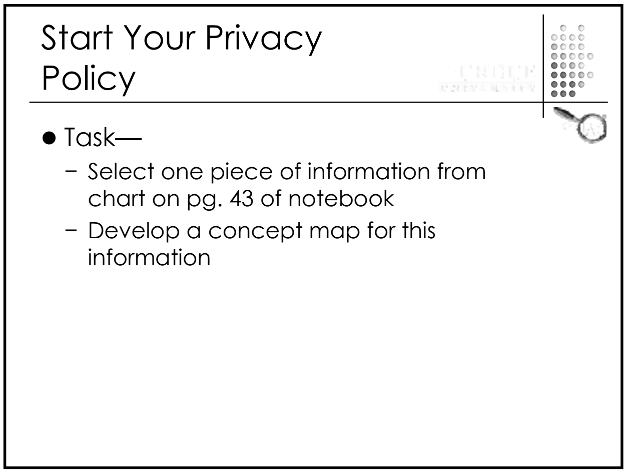
Reminder

- Personally identifiable information gathered should be—
  - Relevant to purpose for gathered
  - Accurate
  - Complete
  - Meaningful
  - Current

Student Health Information Example

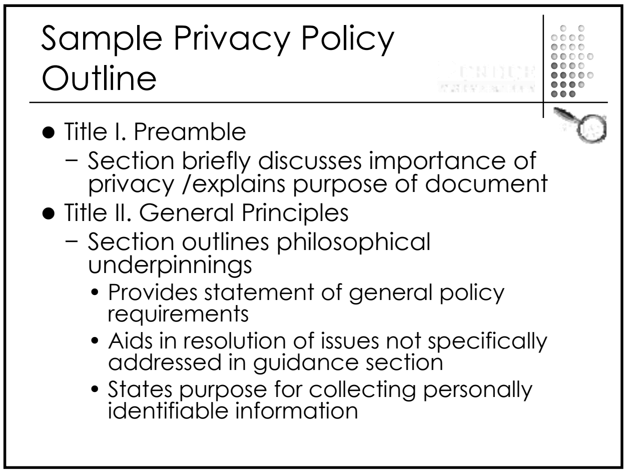

Student Health Information
Provided by Parent/ Doctor/ Student
Input in Student Info System by Secretary
Provided to Nurse
Decision as to whether to provide to staff
Yes, put on building shared drive
No-- remains in SIS
May be also put in team folder on shared ...
Teachers may put in gradebook, database in home directory ...
Teacher may transfer gradebook information to home computer used by other family members

- Why would info be provided?
- Who makes decision on ability to see information?
- How is information secured?
  - Example is on pg. 45 of notebook



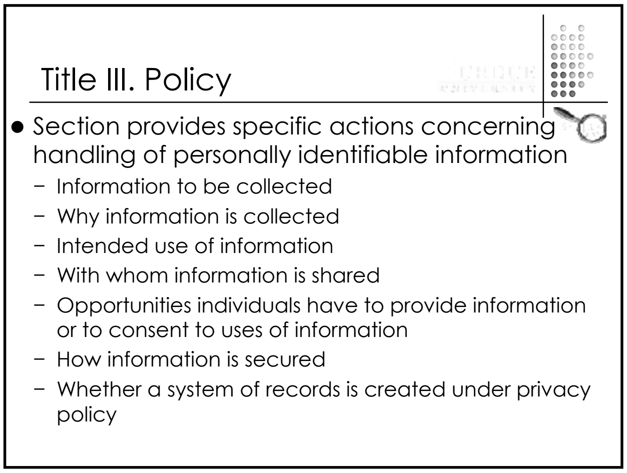
Start Your Privacy Policy

- Task—
  - Select one piece of information from chart on pg. 43 of notebook
  - Develop a concept map for this information



Sample Privacy Policy Outline

- Title I. Preamble
  - Section briefly discusses importance of privacy /explains purpose of document
- Title II. General Principles
  - Section outlines philosophical underpinnings
    - Provides statement of general policy requirements
    - Aids in resolution of issues not specifically addressed in guidance section
    - States purpose for collecting personally identifiable information



Title III. Policy

- Section provides specific actions concerning handling of personally identifiable information
  - Information to be collected
  - Why information is collected
  - Intended use of information
  - With whom information is shared
  - Opportunities individuals have to provide information or to consent to uses of information
  - How information is secured
  - Whether a system of records is created under privacy policy

Title IV. Accountability and Transparency

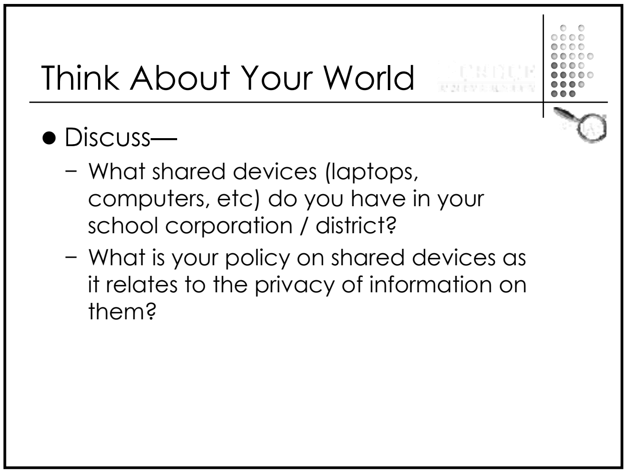
- Section provides information on—
  - Openness of information management practices
  - Remedies available under law for information collected
  - Any audits conducted for compliance
  - Any processes in place for correction of information.

Continue Your Privacy Policy

- Begin developing this section of your policy based on your concept map
  - See example on pg. 46 of notebook

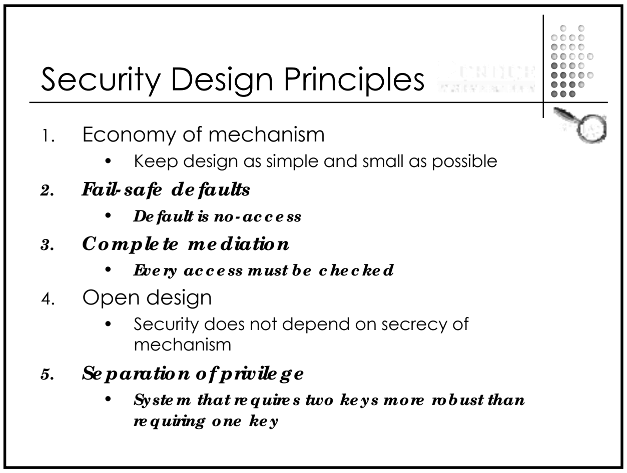
Learn About—

- Using Security Tools for Privacy Protection



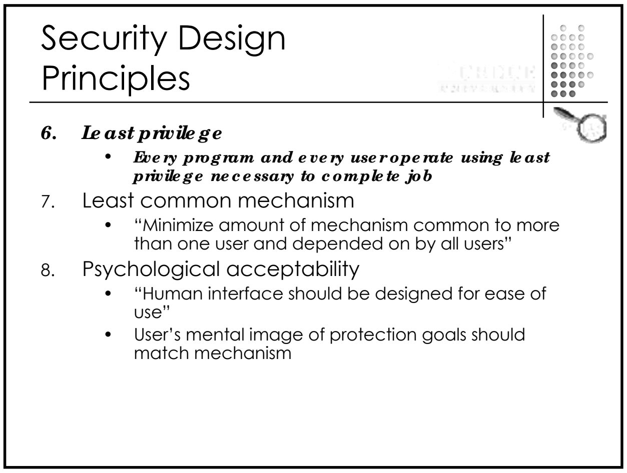
Think About Your World

- Discuss—
  - What shared devices (laptops, computers, etc) do you have in your school corporation / district?
  - What is your policy on shared devices as it relates to the privacy of information on them?



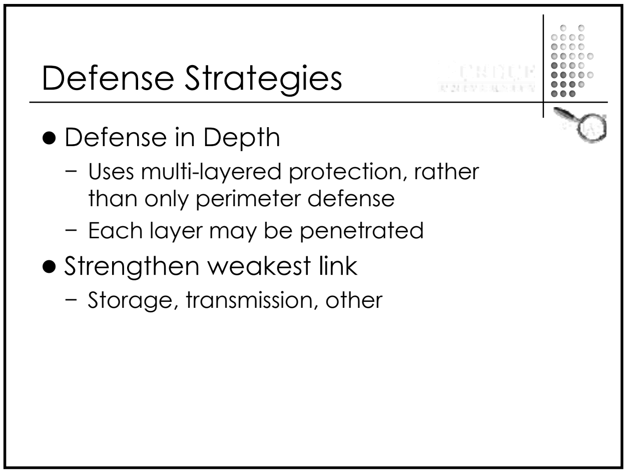
Security Design Principles

1. Economy of mechanism
   - Keep design as simple and small as possible
2. ***Fail-safe defaults***
   - ***Default is no-access***
3. ***Complete mediation***
   - ***Every access must be checked***
4. Open design
   - Security does not depend on secrecy of mechanism
5. ***Separation of privilege***
   - ***System that requires two keys more robust than requiring one key***



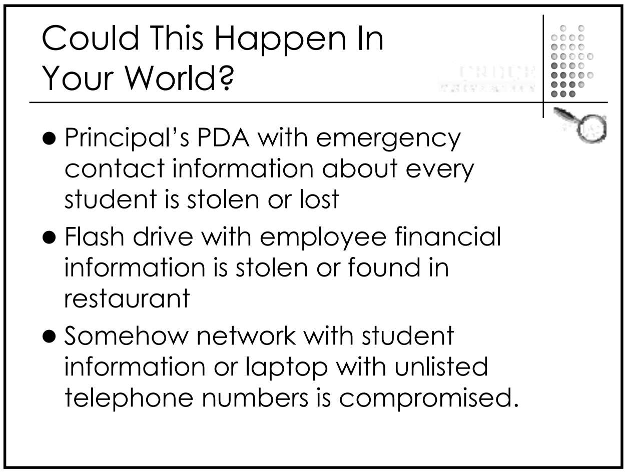
Security Design Principles

6. ***Least privilege***
   - ***Every program and every user operate using least privilege necessary to complete job***
7. Least common mechanism
   - “Minimize amount of mechanism common to more than one user and depended on by all users”
8. Psychological acceptability
   - “Human interface should be designed for ease of use”
   - User’s mental image of protection goals should match mechanism



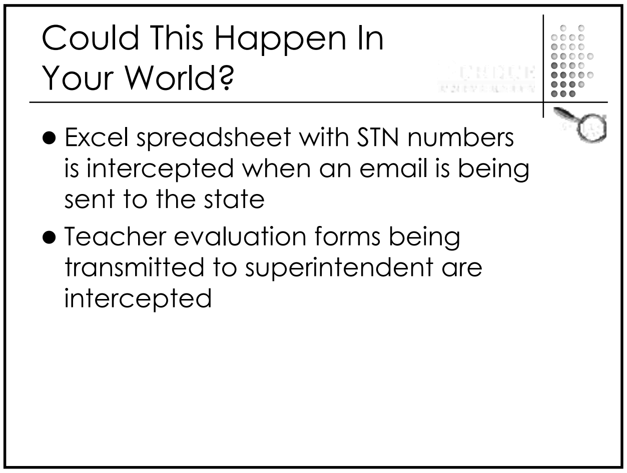
Defense Strategies

- Defense in Depth
  - Uses multi-layered protection, rather than only perimeter defense
  - Each layer may be penetrated
- Strengthen weakest link
  - Storage, transmission, other



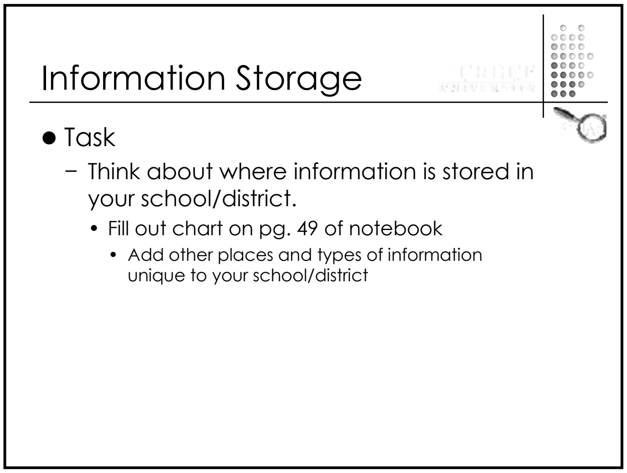
Could This Happen In Your World?

- Principal’s PDA with emergency contact information about every student is stolen or lost
- Flash drive with employee financial information is stolen or found in restaurant
- Somehow network with student information or laptop with unlisted telephone numbers is compromised.



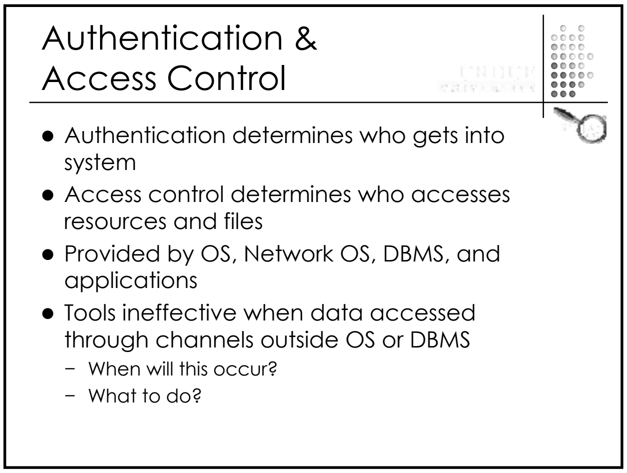
Could This Happen In Your World?

- Excel spreadsheet with STN numbers is intercepted when an email is being sent to the state
- Teacher evaluation forms being transmitted to superintendent are intercepted



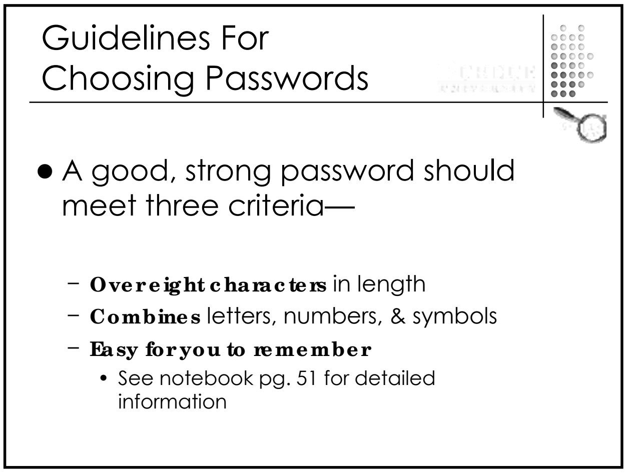
Information Storage

- Task
  - Think about where information is stored in your school/district.
    - Fill out chart on pg. 49 of notebook
      - Add other places and types of information unique to your school/district



Authentication & Access Control

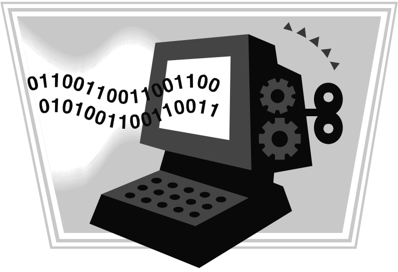
- Authentication determines who gets into system
- Access control determines who accesses resources and files
- Provided by OS, Network OS, DBMS, and applications
- Tools ineffective when data accessed through channels outside OS or DBMS
  - When will this occur?
  - What to do?



Guidelines For Choosing Passwords

- A good, strong password should meet three criteria—
  - **Overeight characters** in length
  - **Combines** letters, numbers, & symbols
  - **Easy foryou to remember**
    - See notebook pg. 51 for detailed information

Cryptography in Five Slides

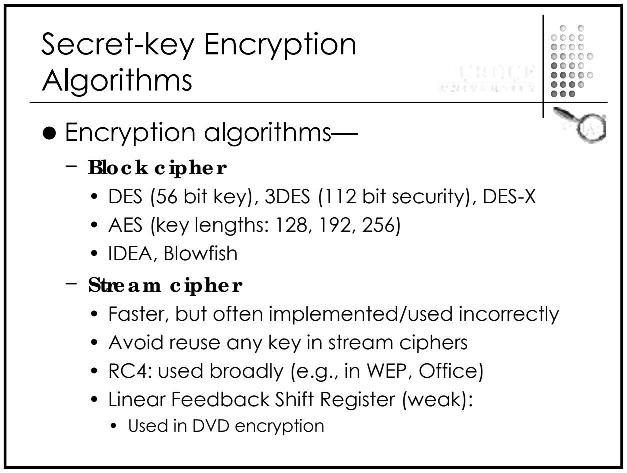


Terminologies

- Cryptography = *kryptos* (hidden) + *graphia* (writing)
- Cryptology = cryptography + cryptanalysis
- Goals of cryptography:
  - Confidentiality, secrecy (by encryption)
  - Integrity, authenticity
- Two main kinds of cryptography
  - Secret-key based algorithms
  - Public-key based algorithms

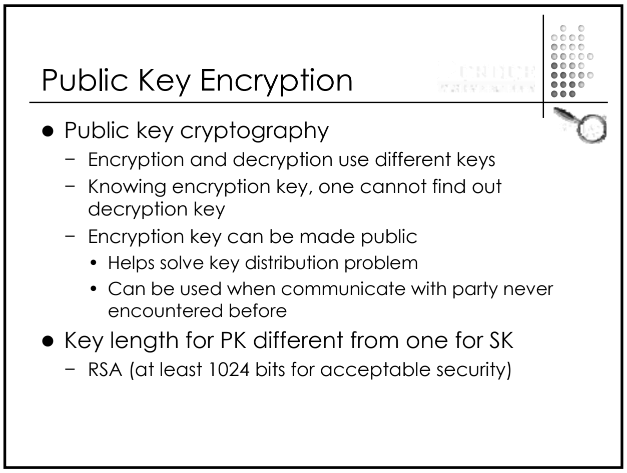
Secret-Key Cryptography

- Encryption/decryption uses the same key
  - Key kept secret
  - Key distribution challenging
- Strength of encryption determined by—
  - Strength of the algorithm
    - Trust only well-known algorithms
  - Length of the key (# of bits)
    - 40 bit key takes hours to break using commodity hardware/software
    - 80 bit for minimal level of security



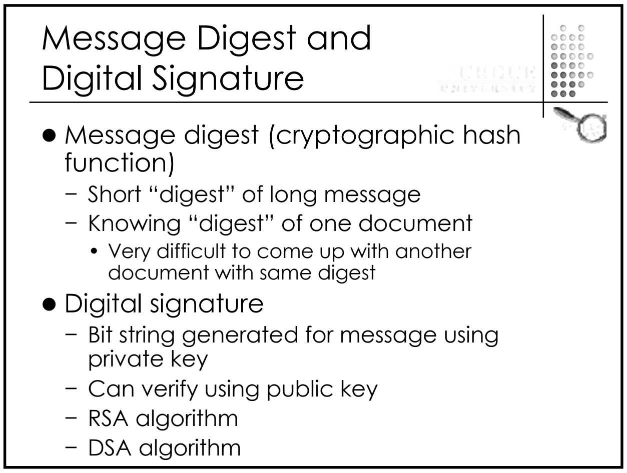
Secret-key Encryption Algorithms

- Encryption algorithms—
  - **Block cipher**
    - DES (56 bit key), 3DES (112 bit security), DES-X
    - AES (key lengths: 128, 192, 256)
    - IDEA, Blowfish
  - **Stream cipher**
    - Faster, but often implemented/used incorrectly
    - Avoid reuse any key in stream ciphers
    - RC4: used broadly (e.g., in WEP, Office)
    - Linear Feedback Shift Register (weak):
      - Used in DVD encryption



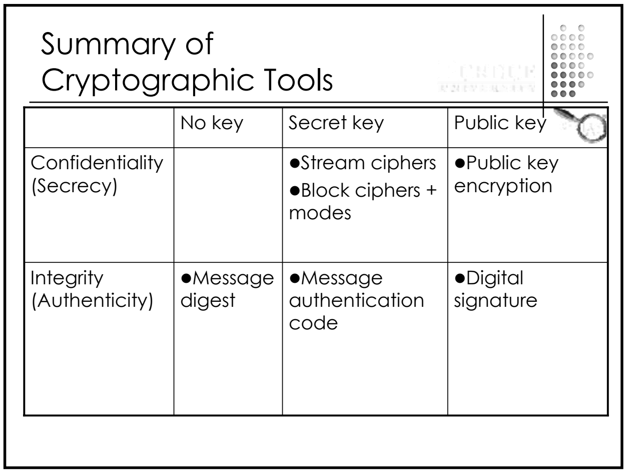
Public Key Encryption

- Public key cryptography
  - Encryption and decryption use different keys
  - Knowing encryption key, one cannot find out decryption key
  - Encryption key can be made public
    - Helps solve key distribution problem
    - Can be used when communicate with party never encountered before
- Key length for PK different from one for SK
  - RSA (at least 1024 bits for acceptable security)



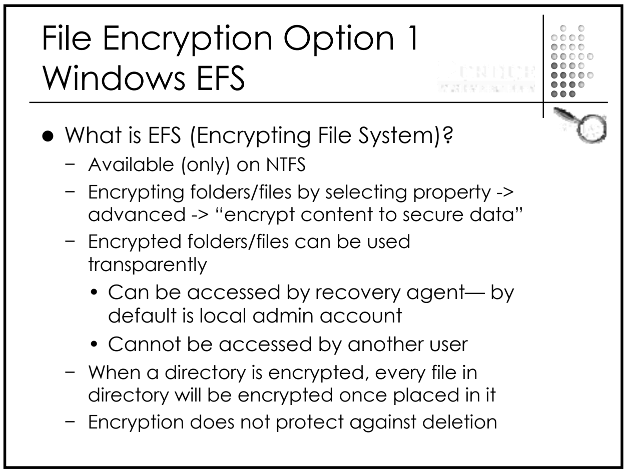
Message Digest and Digital Signature

- Message digest (cryptographic hash function)
  - Short "digest" of long message
  - Knowing "digest" of one document
    - Very difficult to come up with another document with same digest
- Digital signature
  - Bit string generated for message using private key
  - Can verify using public key
  - RSA algorithm
  - DSA algorithm



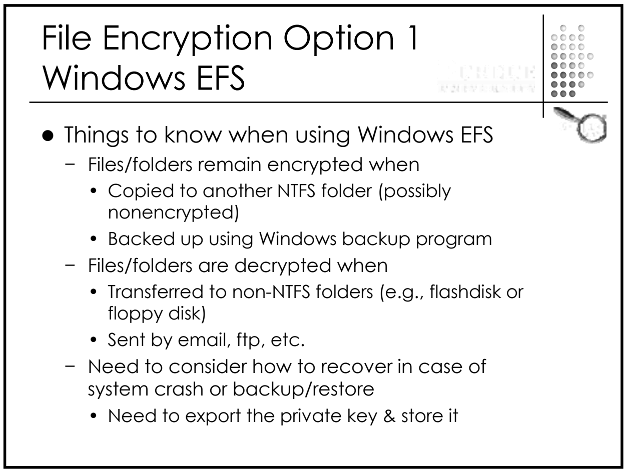
Summary of Cryptographic Tools

	No key	Secret key	Public key
Confidentiality (Secrecy)		●Stream ciphers ●Block ciphers + modes	●Public key encryption
Integrity (Authenticity)	●Message digest	●Message authentication code	●Digital signature



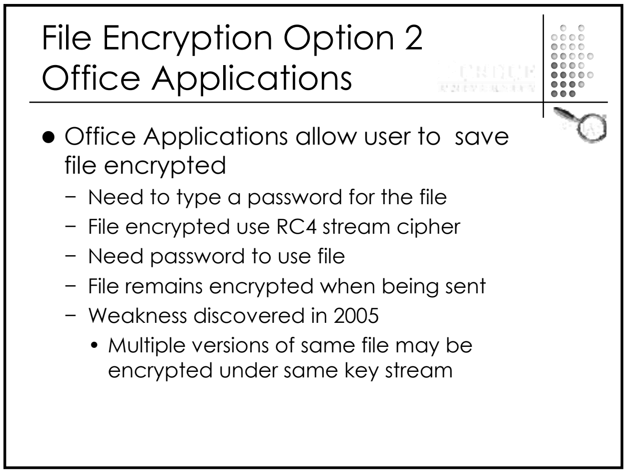
File Encryption Option 1 Windows EFS

- What is EFS (Encrypting File System)?
  - Available (only) on NTFS
  - Encrypting folders/files by selecting property -> advanced -> "encrypt content to secure data"
  - Encrypted folders/files can be used transparently
    - Can be accessed by recovery agent— by default is local admin account
    - Cannot be accessed by another user
  - When a directory is encrypted, every file in directory will be encrypted once placed in it
  - Encryption does not protect against deletion



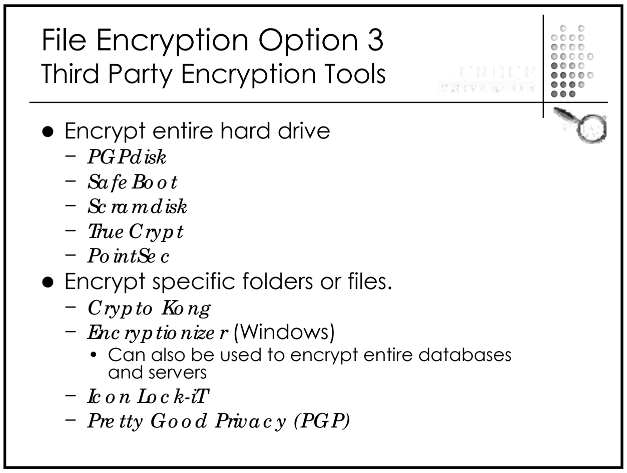
File Encryption Option 1 Windows EFS

- Things to know when using Windows EFS
  - Files/folders remain encrypted when
    - Copied to another NTFS folder (possibly nonencrypted)
    - Backed up using Windows backup program
  - Files/folders are decrypted when
    - Transferred to non-NTFS folders (e.g., flashdisk or floppy disk)
    - Sent by email, ftp, etc.
  - Need to consider how to recover in case of system crash or backup/restore
    - Need to export the private key & store it



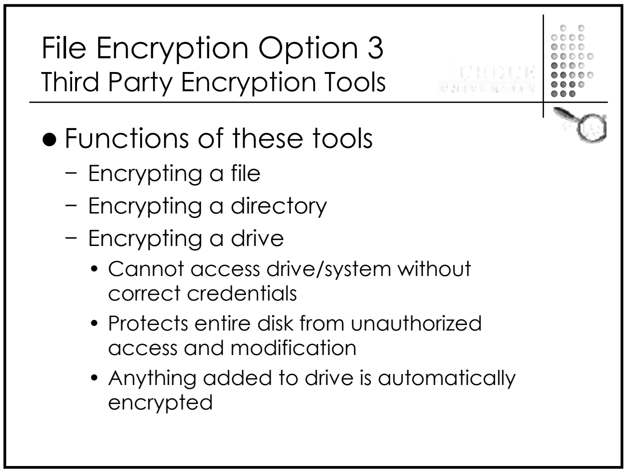
File Encryption Option 2
Office Applications

- Office Applications allow user to save file encrypted
  - Need to type a password for the file
  - File encrypted use RC4 stream cipher
  - Need password to use file
  - File remains encrypted when being sent
  - Weakness discovered in 2005
    - Multiple versions of same file may be encrypted under same key stream



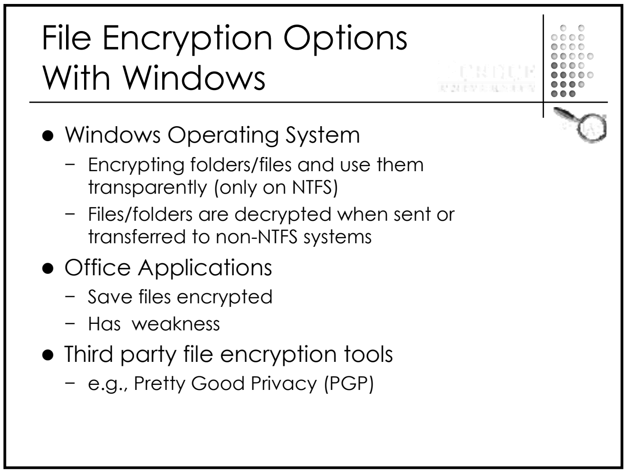
File Encryption Option 3
Third Party Encryption Tools

- Encrypt entire hard drive
  - *PGPdisk*
  - *SafeBoot*
  - *Scramdisk*
  - *TrueCrypt*
  - *PointSec*
- Encrypt specific folders or files.
  - *Crypto Kong*
  - *Encryptionizer* (Windows)
    - Can also be used to encrypt entire databases and servers
  - *Icon Lock-iT*
  - *Pretty Good Privacy (PGP)*



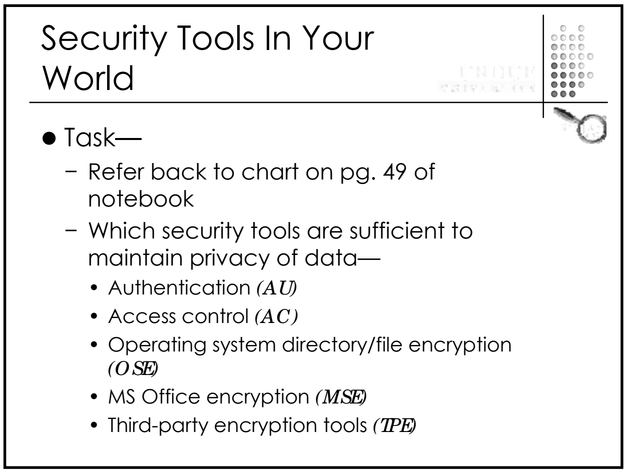
File Encryption Option 3
Third Party Encryption Tools

- Functions of these tools
  - Encrypting a file
  - Encrypting a directory
  - Encrypting a drive
    - Cannot access drive/system without correct credentials
    - Protects entire disk from unauthorized access and modification
    - Anything added to drive is automatically encrypted



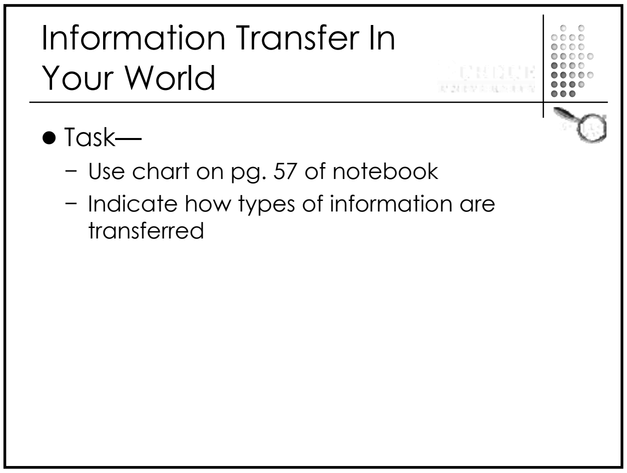
File Encryption Options With Windows

- Windows Operating System
  - Encrypting folders/files and use them transparently (only on NTFS)
  - Files/folders are decrypted when sent or transferred to non-NTFS systems
- Office Applications
  - Save files encrypted
  - Has weakness
- Third party file encryption tools
  - e.g., Pretty Good Privacy (PGP)



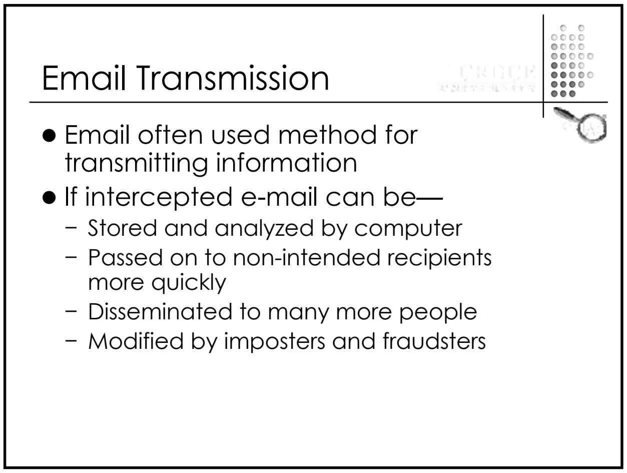
Security Tools In Your World

- Task—
  - Refer back to chart on pg. 49 of notebook
  - Which security tools are sufficient to maintain privacy of data—
    - Authentication *(AU)*
    - Access control *(AC)*
    - Operating system directory/file encryption *(OSE)*
    - MS Office encryption *(MSE)*
    - Third-party encryption tools *(TPE)*



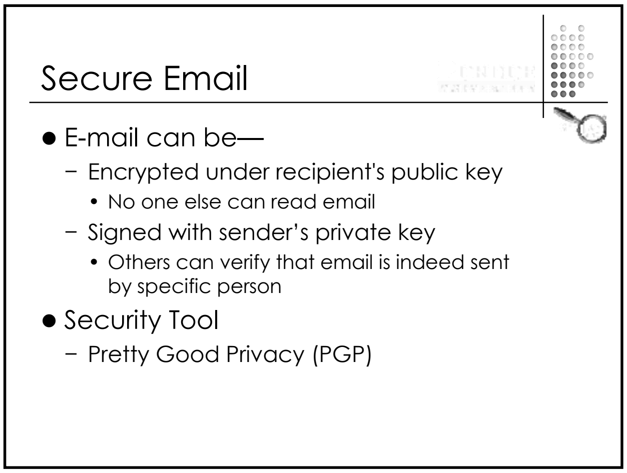
Information Transfer In Your World

- Task—
  - Use chart on pg. 57 of notebook
  - Indicate how types of information are transferred



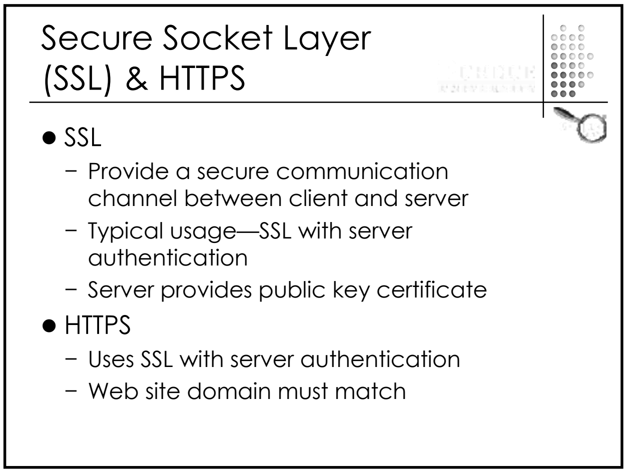
Email Transmission

- Email often used method for transmitting information
- If intercepted e-mail can be—
  - Stored and analyzed by computer
  - Passed on to non-intended recipients more quickly
  - Disseminated to many more people
  - Modified by imposters and fraudsters



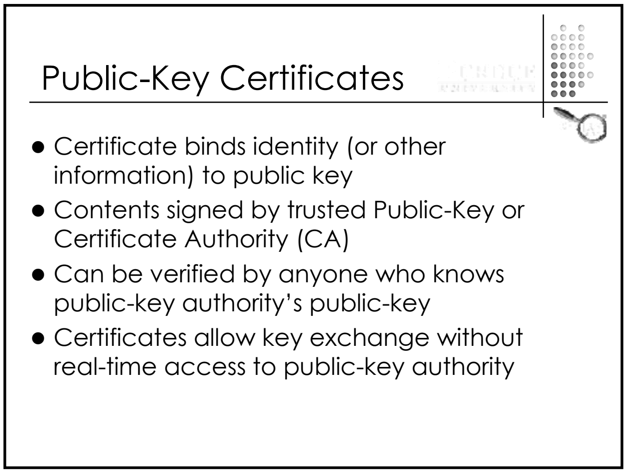
Secure Email

- E-mail can be—
  - Encrypted under recipient's public key
    - No one else can read email
  - Signed with sender’s private key
    - Others can verify that email is indeed sent by specific person
- Security Tool
  - Pretty Good Privacy (PGP)



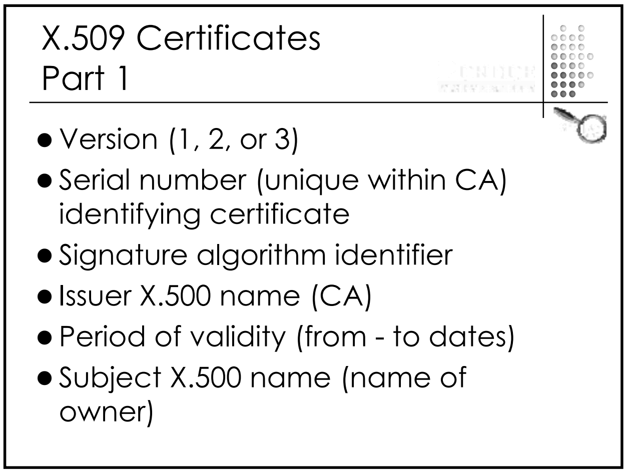
Secure Socket Layer (SSL) & HTTPS

- SSL
  - Provide a secure communication channel between client and server
  - Typical usage—SSL with server authentication
  - Server provides public key certificate
- HTTPS
  - Uses SSL with server authentication
  - Web site domain must match



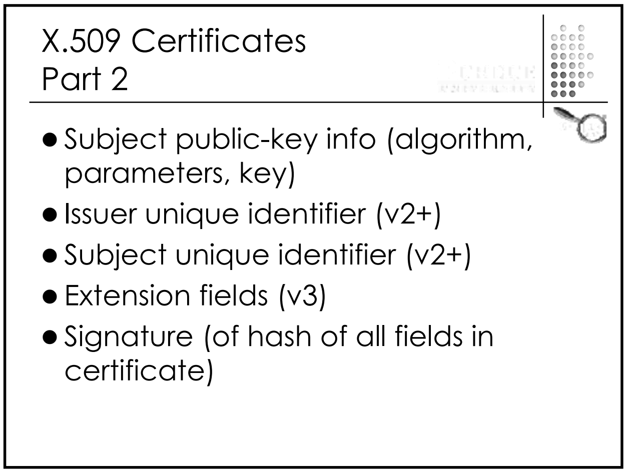
Public-Key Certificates

- Certificate binds identity (or other information) to public key
- Contents signed by trusted Public-Key or Certificate Authority (CA)
- Can be verified by anyone who knows public-key authority's public-key
- Certificates allow key exchange without real-time access to public-key authority



X.509 Certificates Part 1

- Version (1, 2, or 3)
- Serial number (unique within CA) identifying certificate
- Signature algorithm identifier
- Issuer X.500 name (CA)
- Period of validity (from - to dates)
- Subject X.500 name (name of owner)



X.509 Certificates Part 2

- Subject public-key info (algorithm, parameters, key)
- Issuer unique identifier (v2+)
- Subject unique identifier (v2+)
- Extension fields (v3)
- Signature (of hash of all fields in certificate)

How to Obtain a Certificate?

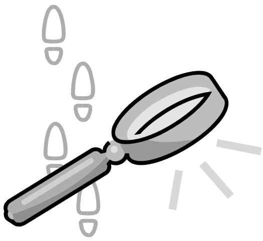
- For particular application can define your own CA
  - Libraries like openssl provide necessary tools
  - Many companies define own CA
- VeriSign—Company provides certificates to many commercial companies
- Private key remains secret and certificate must be accessible
- Example—See certificates accepted by your browser

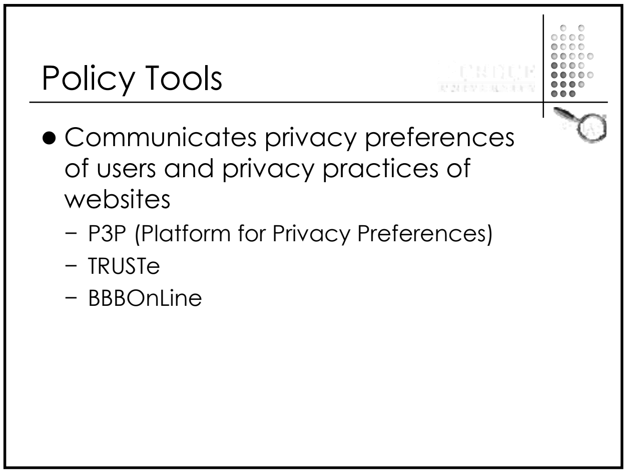
Security Tools In Your World

- Comparison Task
  - When would you want to use a password, access control system or encryption?
    - See pg. 59 for further information

Learn About—

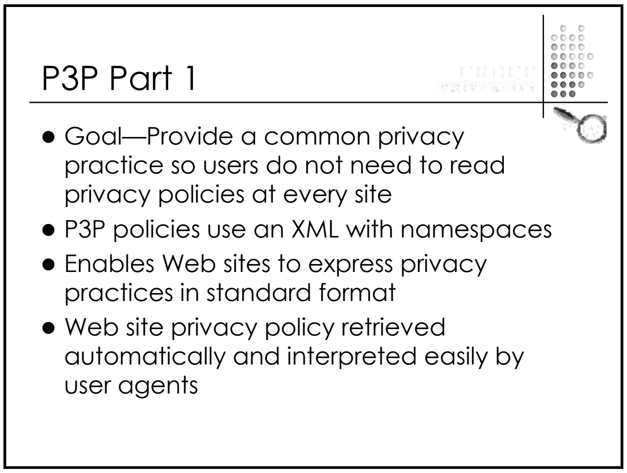
- Privacy Enhancing Technologies (PET) & Practices





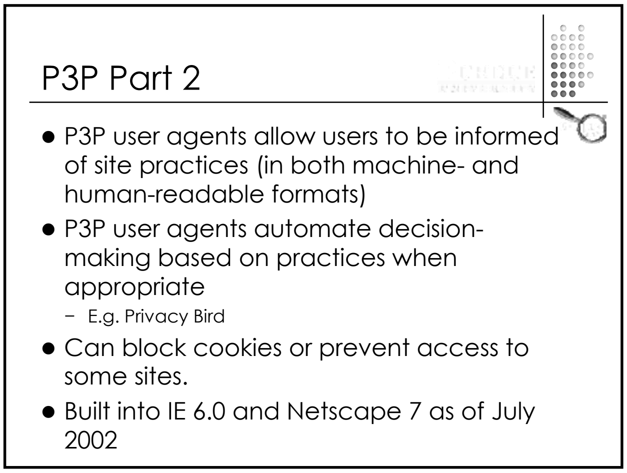
Policy Tools

- Communicates privacy preferences of users and privacy practices of websites
  - P3P (Platform for Privacy Preferences)
  - TRUSTe
  - BBBOnLine



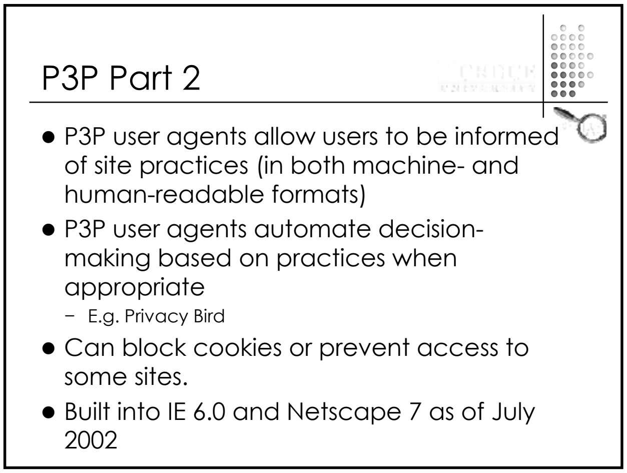
P3P Part 1

- Goal—Provide a common privacy practice so users do not need to read privacy policies at every site
- P3P policies use an XML with namespaces
- Enables Web sites to express privacy practices in standard format
- Web site privacy policy retrieved automatically and interpreted easily by user agents



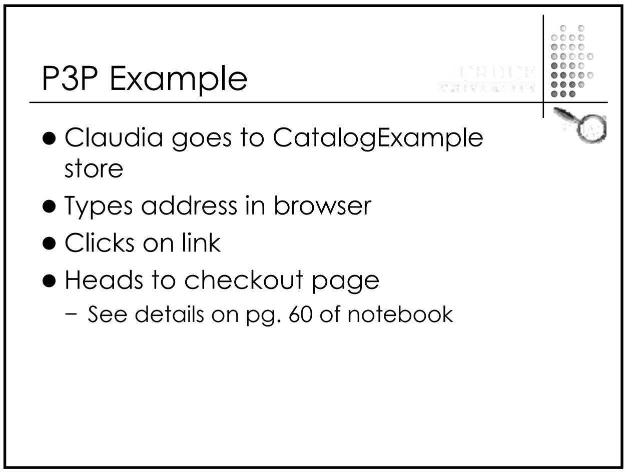
P3P Part 2

- P3P user agents allow users to be informed of site practices (in both machine- and human-readable formats)
- P3P user agents automate decision-making based on practices when appropriate
  - E.g. Privacy Bird
- Can block cookies or prevent access to some sites.
- Built into IE 6.0 and Netscape 7 as of July 2002



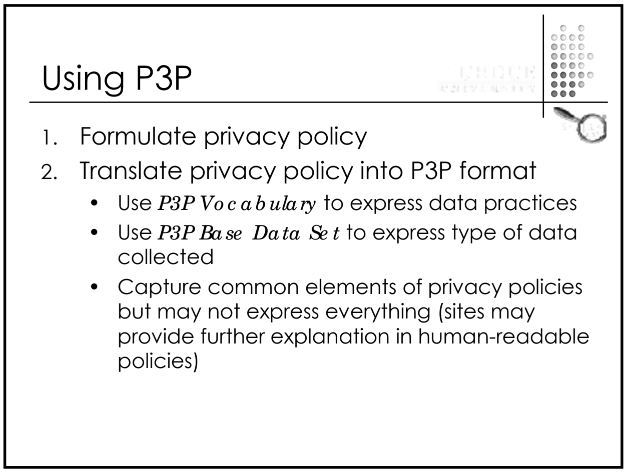
P3P Part 2

- P3P user agents allow users to be informed of site practices (in both machine- and human-readable formats)
- P3P user agents automate decision-making based on practices when appropriate
  - E.g. Privacy Bird
- Can block cookies or prevent access to some sites.
- Built into IE 6.0 and Netscape 7 as of July 2002



P3P Example

- Claudia goes to CatalogExample store
- Types address in browser
- Clicks on link
- Heads to checkout page
  - See details on pg. 60 of notebook



Using P3P

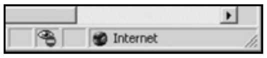
1. Formulate privacy policy
2. Translate privacy policy into P3P format
   - Use *P3P Vocabulary* to express data practices
   - Use *P3P Base Data Set* to express type of data collected
   - Capture common elements of privacy policies but may not express everything (sites may provide further explanation in human-readable policies)

Using P3P Continued

3. Place P3P policy on web site
   - One policy for entire site or multiple policies for different parts of site
4. Associate policy with web resources
   - Place P3P policy reference file (which identifies location of relevant policy file) at well-known location on server
   - Configure server to insert P3P header with link to P3P policy reference file
   - Insert link to P3P policy reference file in HTML content

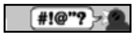
Internet Explorer 6.0

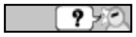
- User may see warning appear—
  - When browser encounters a cookie not having compact P3P policy
  - When encounters P3P policy does not match privacy preferences set in IE 6.0 under the Privacy tab in Internet Options pull-down menu

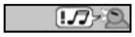


AT&T Privacy Bird

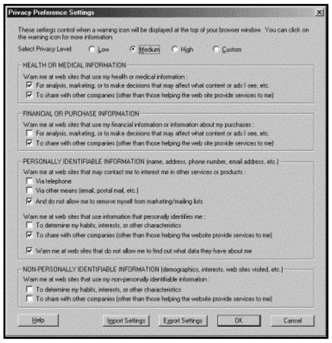
- Displays a bird icon in top right of user's browser title bar
- Displays different color of bird to indicate whether or not website P3P policy matches user’s preferences
- Can be configured to provide audible chirp as warning







AT&T Privacy Bird Settings



Privacy Preference Settings

These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

Select Privacy Level ○ Low ● Medium ○ High ○ Custom

HEALTH OR MEDICAL INFORMATION

Warn me at web sites that use my health or medical information :

- ☑ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☑ To share with other companies (other than those helping the web site provide services to me)

FINANCIAL OR PURCHASE INFORMATION

Warn me at web sites that use my financial information or information about my purchases :

- □ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☑ To share with other companies (other than those helping the web site provide services to me)

PERSONALLY IDENTIFIABLE INFORMATION (name, address, phone number, email address, etc.)

Warn me at web sites that may contact me to interest me in other services or products :

- □ Via telephone
- □ Via other means (email, postal mail, etc.)
- ☑ And do not allow me to remove myself from marketing/mailing lists

Warn me at web sites that use information that personally identifies me :

- □ To determine my habits, interests, or other characteristics
- ☑ To share with other companies (other than those helping the website provide services to me)

☑ Warn me at web sites that do not allow me to find out what data they have about me

NON-PERSONALLY IDENTIFIABLE INFORMATION (demographics, interests, web sites visited, etc.)

Warn me at web sites that use my non-personally identifiable information :

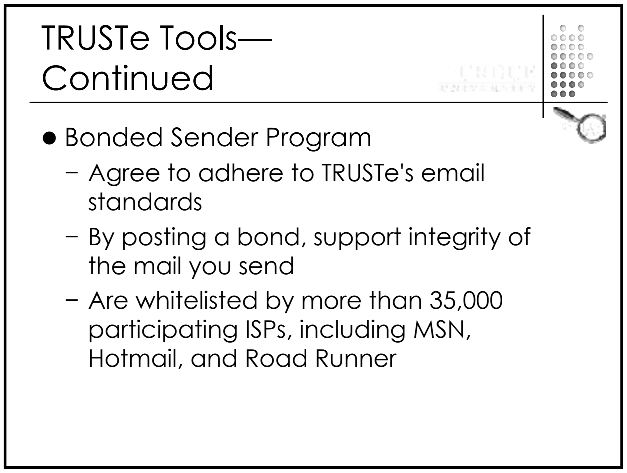
- □ To determine my habits, interests, or other characteristics
- □ To share with other companies (other than those helping the website provide services to me)

TRUSTe

- Independent, nonprofit organization
  - Goal—
    - Enable trust based on privacy for personal information on Internet
- Certify and monitor web site privacy and email policies
- Monitor practices of organizations regarding privacy
- Resolve thousands of consumer privacy problems every year

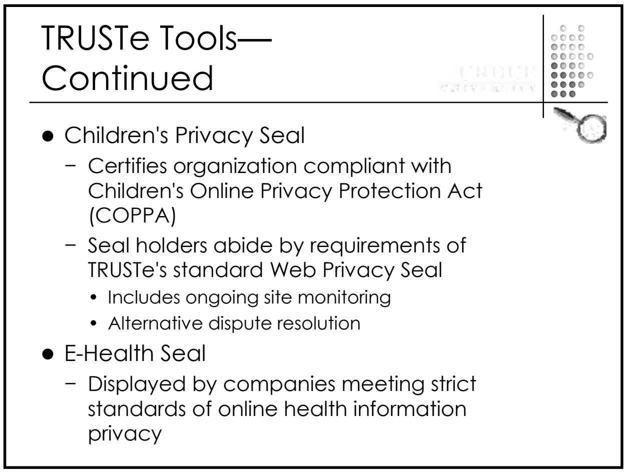
TRUSTe Tools

- Web Privacy Seal
  - Displaying TRUSTe seal demonstrates site complies with best practices
- Email Privacy Seal
  - **"We Don't Spam" seal** certifies businesses by implementing a rigorous review process, including an initial self-assessment of email practices by sender, analysis by TRUSTe, and review of sender's email abuse history



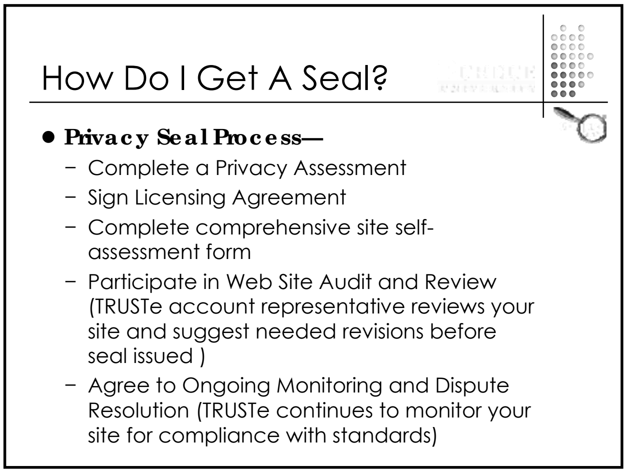
TRUSTe Tools—Continued

- Bonded Sender Program
  - Agree to adhere to TRUSTe's email standards
  - By posting a bond, support integrity of the mail you send
  - Are whitelisted by more than 35,000 participating ISPs, including MSN, Hotmail, and Road Runner



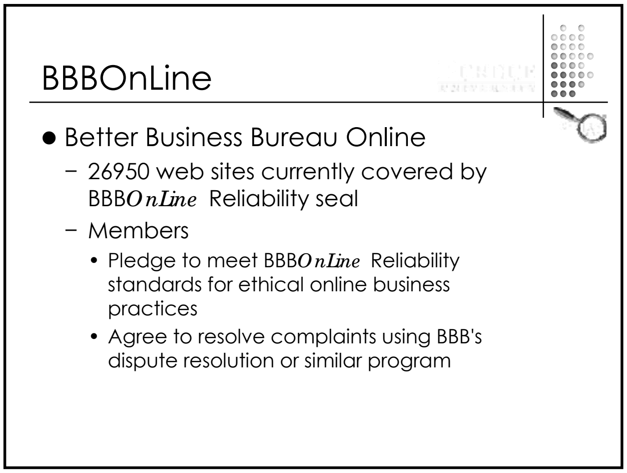
TRUSTe Tools—Continued

- Children's Privacy Seal
  - Certifies organization compliant with Children's Online Privacy Protection Act (COPPA)
  - Seal holders abide by requirements of TRUSTe's standard Web Privacy Seal
    - Includes ongoing site monitoring
    - Alternative dispute resolution
- E-Health Seal
  - Displayed by companies meeting strict standards of online health information privacy



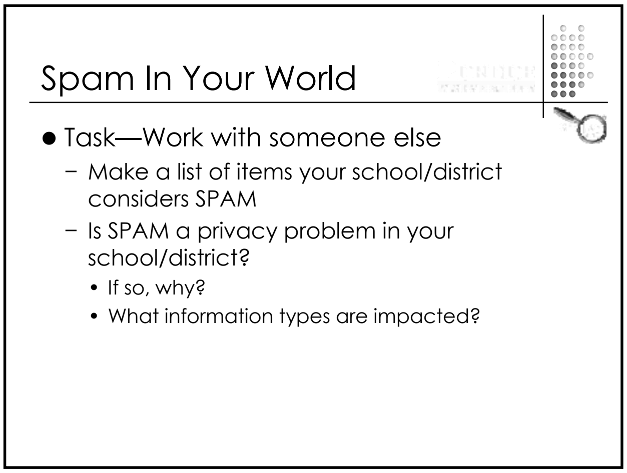
How Do I Get A Seal?

- **Privacy Seal Process—**
  - Complete a Privacy Assessment
  - Sign Licensing Agreement
  - Complete comprehensive site self-assessment form
  - Participate in Web Site Audit and Review (TRUSTe account representative reviews your site and suggest needed revisions before seal issued)
  - Agree to Ongoing Monitoring and Dispute Resolution (TRUSTe continues to monitor your site for compliance with standards)



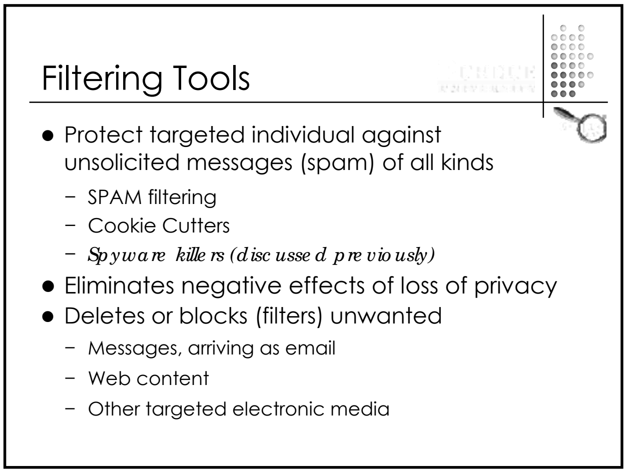
BBBOnLine

- Better Business Bureau Online
  - 26950 web sites currently covered by BBB*OnLine* Reliability seal
  - Members
    - Pledge to meet BBB*OnLine* Reliability standards for ethical online business practices
    - Agree to resolve complaints using BBB's dispute resolution or similar program



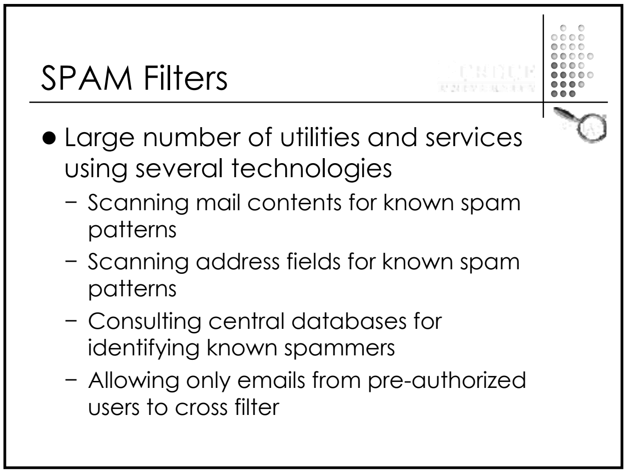
Spam In Your World

- Task—Work with someone else
  - Make a list of items your school/district considers SPAM
  - Is SPAM a privacy problem in your school/district?
    - If so, why?
    - What information types are impacted?



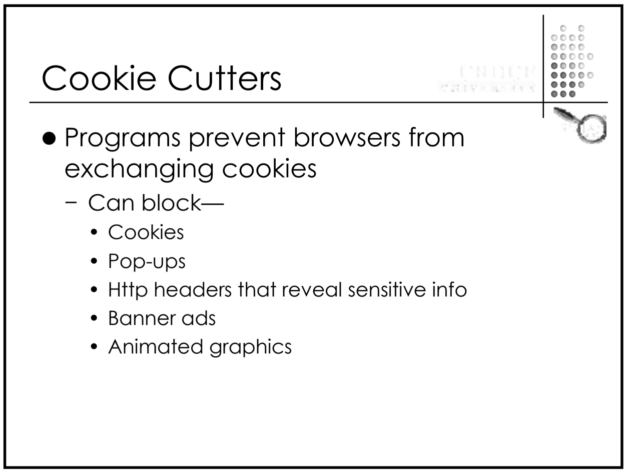
Filtering Tools

- Protect targeted individual against unsolicited messages (spam) of all kinds
  - SPAM filtering
  - Cookie Cutters
  - *Spyware killers (discussed previously)*
- Eliminates negative effects of loss of privacy
- Deletes or blocks (filters) unwanted
  - Messages, arriving as email
  - Web content
  - Other targeted electronic media



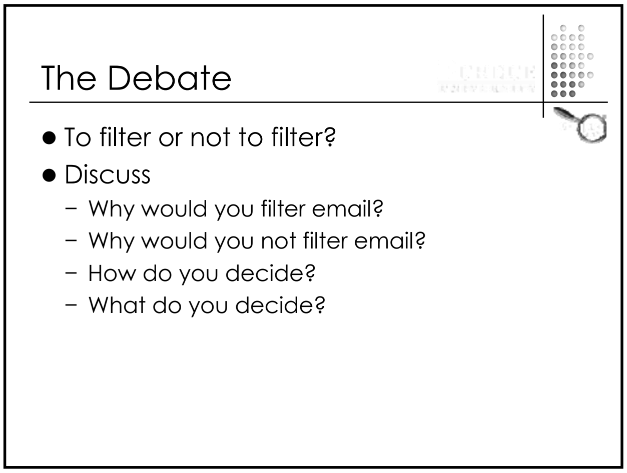
SPAM Filters

- Large number of utilities and services using several technologies
  - Scanning mail contents for known spam patterns
  - Scanning address fields for known spam patterns
  - Consulting central databases for identifying known spammers
  - Allowing only emails from pre-authorized users to cross filter



Cookie Cutters

- Programs prevent browsers from exchanging cookies
  - Can block—
    - Cookies
    - Pop-ups
    - Http headers that reveal sensitive info
    - Banner ads
    - Animated graphics



The Debate

- To filter or not to filter?
- Discuss
  - Why would you filter email?
  - Why would you not filter email?
  - How do you decide?
  - What do you decide?

Anonymizing Tools

(Another Privacy Conundrum)

- Enable users to communicate anonymously
  - Masks IP address and personal info
  - Masks source of email messages
- Strips off user info and sends it to websites
  - Internet Anonymizers
  - Anonymous email (remailers)

Anonymizing Tools—Cont'd

- **Internet Anonymizers**
  - Establish a secure connection on system
- *Networked Anonymizers*
  - Type of anonymizer transfers your communications through network of Internet computers between you and destination
    - Example—
      - Request to visit web page might first go through computers A, B, and C before going to web site
      - Resulting page transferred back though C, B, and A then to you

Anonymizing Tools—Continued

- *Single-point anonymizers*
  - Type of anonymizer passes your surfing through a single web site to protect your identify
  - Often offers an encrypted communications channel for passage of results back to user

Anonymizing Tools—Continued

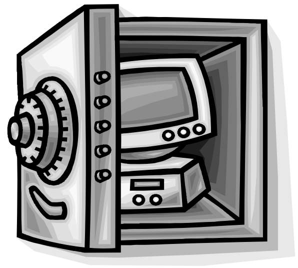
- Anonymous email (remailers)
  - Anonymous remailers allow people to send email without showing identity
  - Similar to anonymous web proxies
    - Send mail to remailer, which strips out any identifying information (very controversial)
    - Remailer forwards message to destination

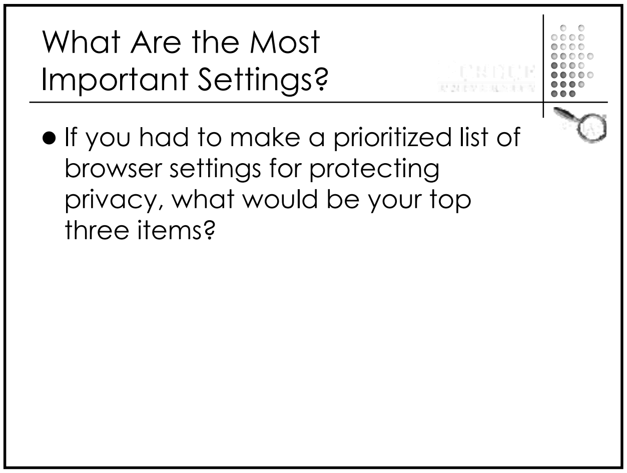
Discussion

- What can anonymizing tools do to protect privacy?
- What are the tradeoffs?

Learn About—

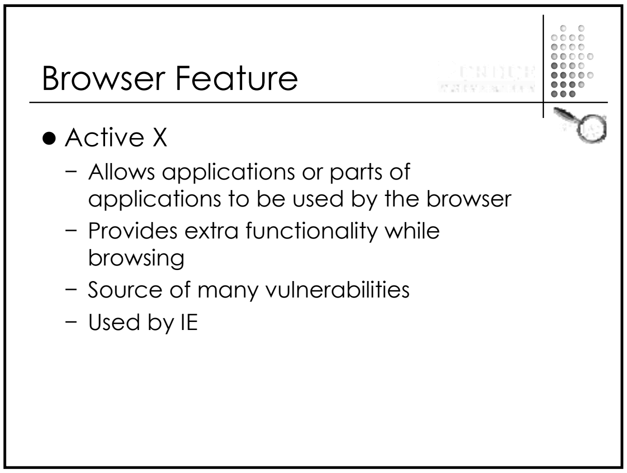
- Browser Settings





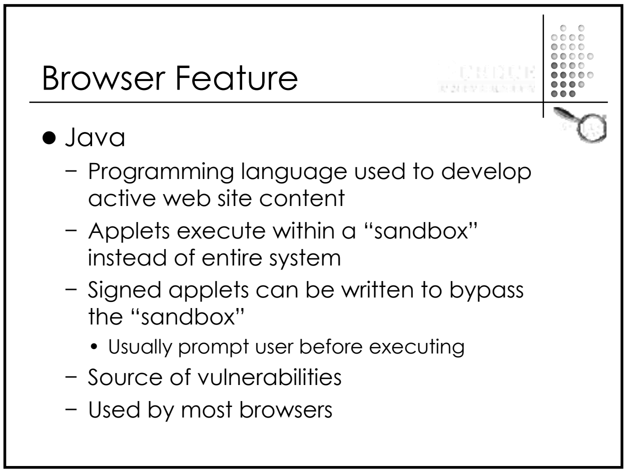
What Are the Most Important Settings?

- If you had to make a prioritized list of browser settings for protecting privacy, what would be your top three items?



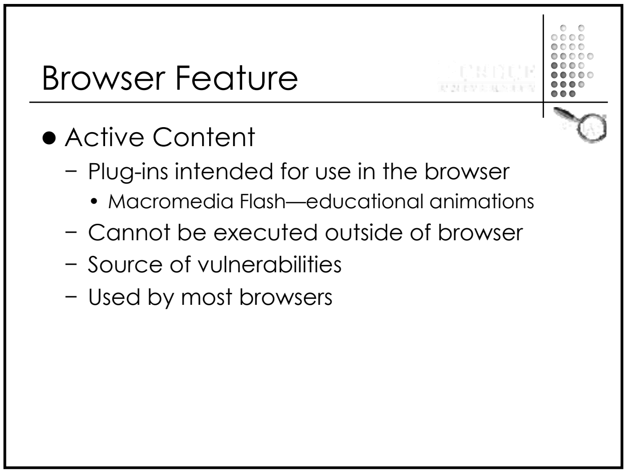
Browser Feature

- Active X
  - Allows applications or parts of applications to be used by the browser
  - Provides extra functionality while browsing
  - Source of many vulnerabilities
  - Used by IE



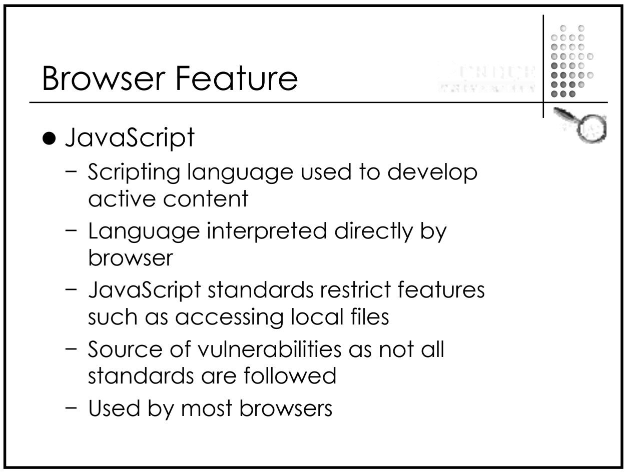
Browser Feature

- Java
  - Programming language used to develop active web site content
  - Applets execute within a "sandbox" instead of entire system
  - Signed applets can be written to bypass the "sandbox"
    - Usually prompt user before executing
  - Source of vulnerabilities
  - Used by most browsers



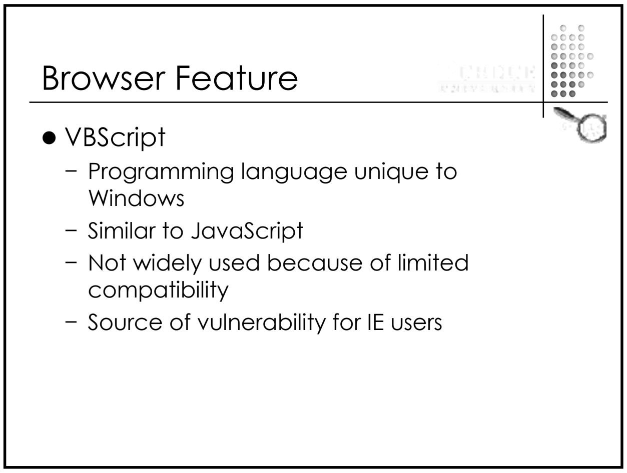
Browser Feature

- Active Content
  - Plug-ins intended for use in the browser
    - Macromedia Flash—educational animations
  - Cannot be executed outside of browser
  - Source of vulnerabilities
  - Used by most browsers



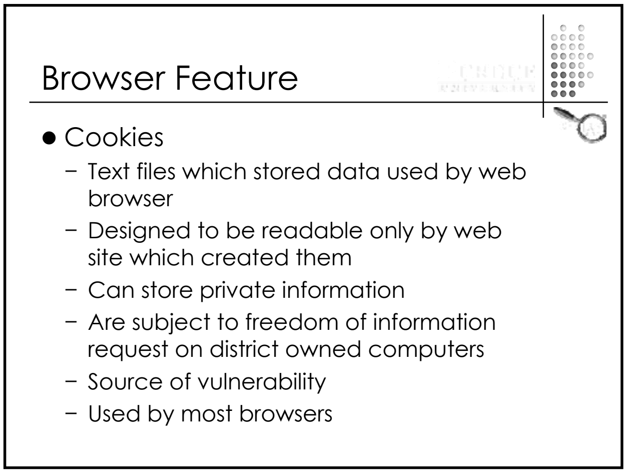
Browser Feature

- JavaScript
  - Scripting language used to develop active content
  - Language interpreted directly by browser
  - JavaScript standards restrict features such as accessing local files
  - Source of vulnerabilities as not all standards are followed
  - Used by most browsers



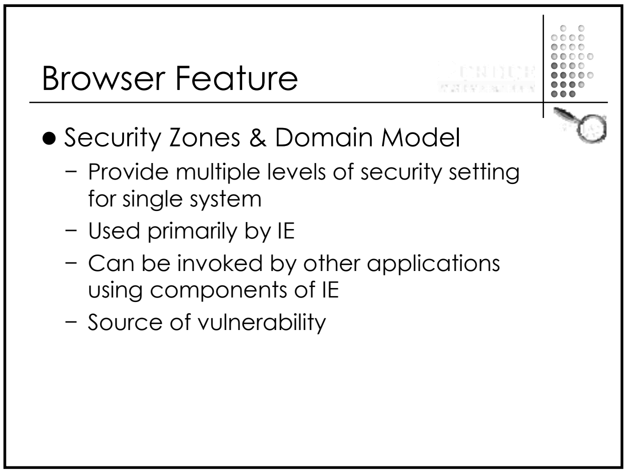
Browser Feature

- VBScript
  - Programming language unique to Windows
  - Similar to JavaScript
  - Not widely used because of limited compatibility
  - Source of vulnerability for IE users



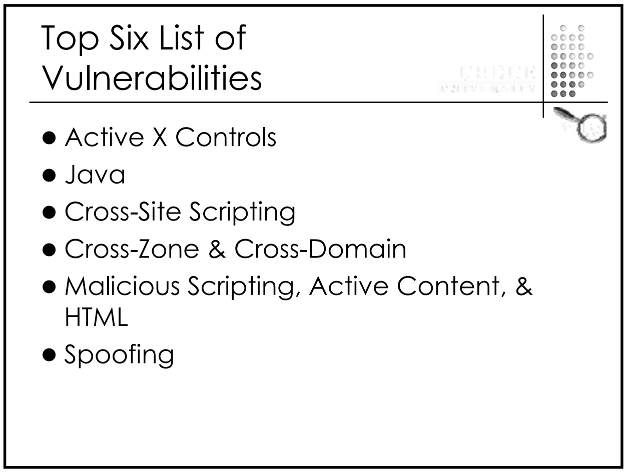
Browser Feature

- Cookies
  - Text files which stored data used by web browser
  - Designed to be readable only by web site which created them
  - Can store private information
  - Are subject to freedom of information request on district owned computers
  - Source of vulnerability
  - Used by most browsers



Browser Feature

- Security Zones & Domain Model
  - Provide multiple levels of security setting for single system
  - Used primarily by IE
  - Can be invoked by other applications using components of IE
  - Source of vulnerability

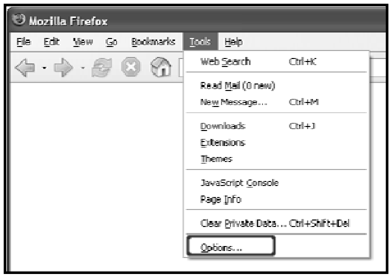


Top Six List of Vulnerabilities

- Active X Controls
- Java
- Cross-Site Scripting
- Cross-Zone & Cross-Domain
- Malicious Scripting, Active Content, & HTML
- Spoofing

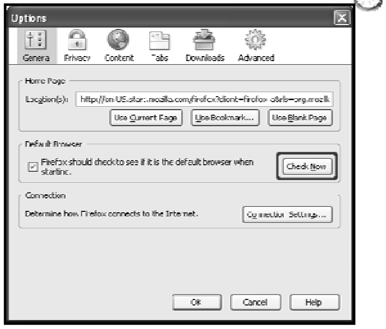
Securing Firefox

- Start with the Tools menu
  - Select Options



General Options

- Select homepage, default browser, connection settings *i.e. use proxy*



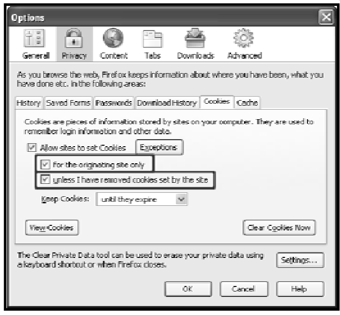
Location(s): http://en-US.start.mozilla.com/firefox?client=firefox-a&rls=org.mozilla

☑ Firefox should check to see if it is the default browser when starting.

Determine how Firefox connects to the Internet.

Privacy Settings

- Enable for original site only
- Enable "unless I have removed cookies set by site"



As you browse the web, Firefox keeps information about where you have been, what you have done etc. in the following areas:

Cookies are pieces of information stored by sites on your computer. They are used to remember login information and other data.

☑ Allow sites to set Cookies

☑ For the originating site only

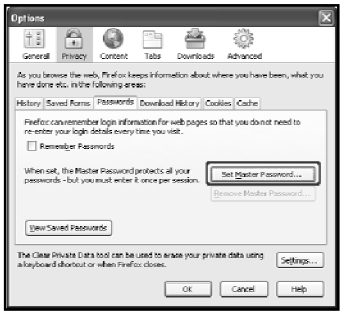
☑ unless I have removed cookies set by the site

Keep Cookies: until they expire

The Clear Private Data tool can be used to erase your private data using a keyboard shortcut or when Firefox closes.

Passwords

- Use Master Password IF you store login information
- This is not a recommended practice



As you browse the web, Firefox keeps information about where you have been, what you have done etc. in the following areas:

Firefox can remember login information for web pages so that you do not need to re-enter your login details every time you visit.

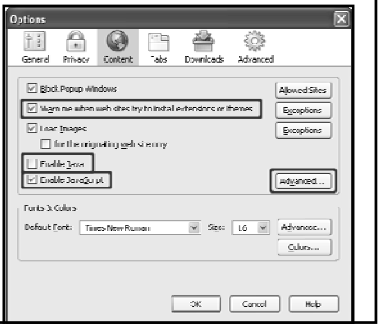
□ Remember Passwords

When set, the Master Password protects all your passwords - but you must enter it once per session.

The Clear Private Data tool can be used to erase your private data using a keyboard shortcut or when Firefox closes.

Content Settings

- Disable Java until you know site is trusted
- Enable to use
- Disable after use
- Warn about installing extensions or themes



☑ Block Popup Windows

☑ Warn me when web sites try to install extensions or themes

☑ Load Images

□ for the originating web site only

□ Enable Java

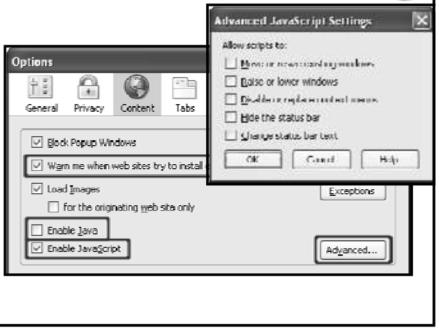
☑ Enable JavaScript

Fonts & Colors

Default Font: Times New Roman Size: 16

Advanced Content Settings

- Enable JavaScript
- Advanced Settings
- Disable all options



☑ Block Popup Windows

☑ Warn me when web sites try to install

☑ Load Images

□ for the originating web site only

□ Enable Java

☑ Enable JavaScript

Allow scripts to:

□ Move or resize existing windows

□ Raise or lower windows

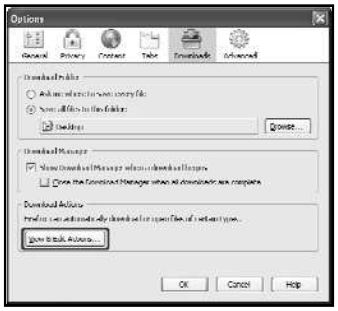
□ Disable or replace context menus

□ Hide the status bar

□ Change status bar text

Download Settings Part 1

- Have files saved
- View & Edit Actions



Download Folder

○ Ask me where to save every file

● Save all files to this folder:

Desktop [Browse...]

Download Manager

☑ Show Download Manager when a download begins

☐ Close the Download Manager when all downloads are complete

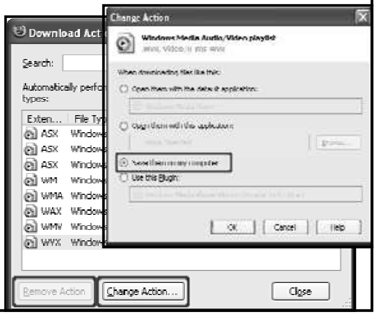
Download Actions

Firefox can automatically download or open files of certain types.

[View & Edit Actions...]

Download Settings Part 2

- Use Change Action
- Do not automatically open files



Search:

Automatically perfo types:

Exten...	File Ty
ASX	Window
ASX	Window
ASX	Window
WM	Window
WMA	Window
WAX	Window
WMV	Window
WVX	Window

Windows Media Audio/Video playlist

When downloading files like this:

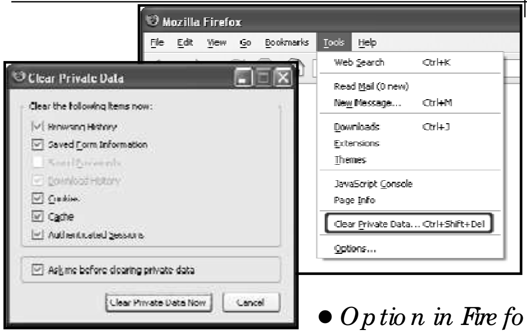
○ Open them with the default application:

○ Open them with this application:

● Save them on my computer

○ Use this Plugin:

Clear Private Data



Clear the following items now:

☑ Browsing History

☑ Saved Form Information

☐ Saved Passwords

☑ Download History

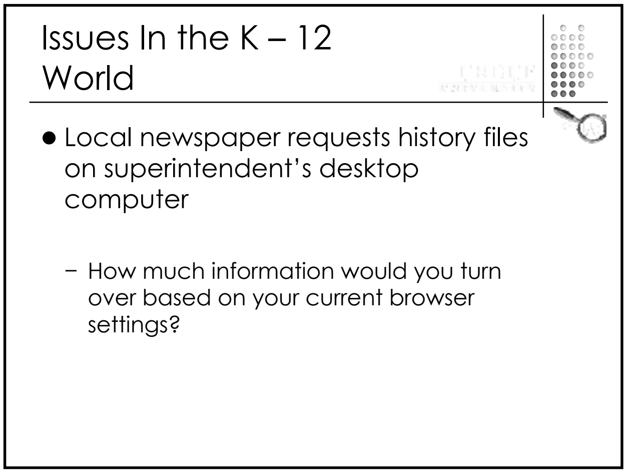
☑ Cookies

☑ Cache

☑ Authenticated Sessions

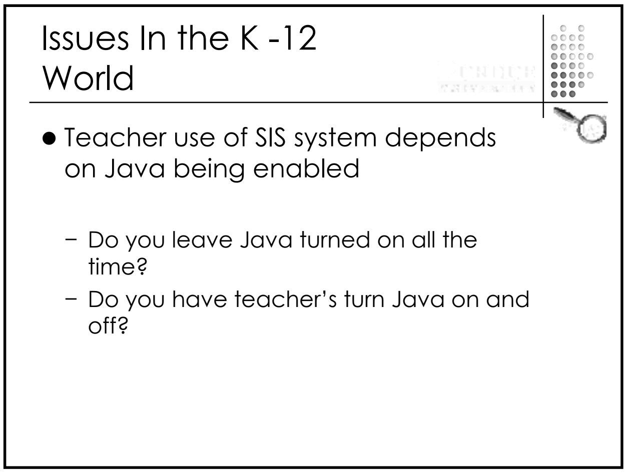
☑ Ask me before clearing private data

- *Option in Firefox 1.5*



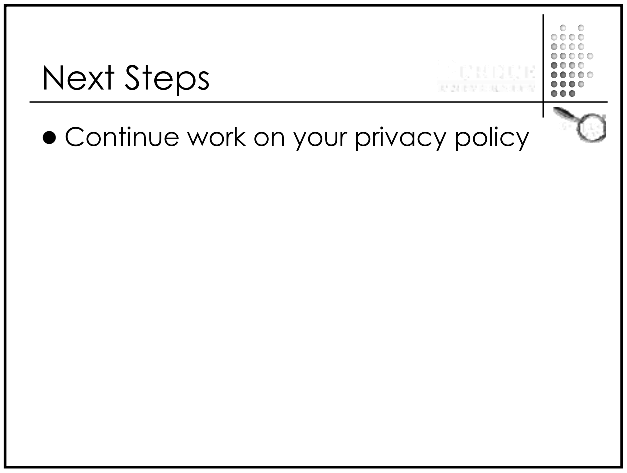
Issues In the K – 12 World

- Local newspaper requests history files on superintendent’s desktop computer
  - How much information would you turn over based on your current browser settings?



Issues In the K -12 World

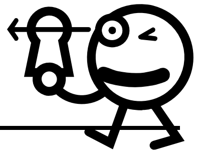
- Teacher use of SIS system depends on Java being enabled
  - Do you leave Java turned on all the time?
  - Do you have teacher’s turn Java on and off?



Next Steps

- Continue work on your privacy policy

Perfect Malware Removal Tool



Brainstorm Characteristics—

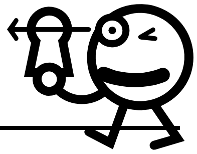
Rank Order Characteristics—

Malware Removal Tool Review

Tool Name:____

Criteria	***Findings***

What Is A Good Privacy Policy?



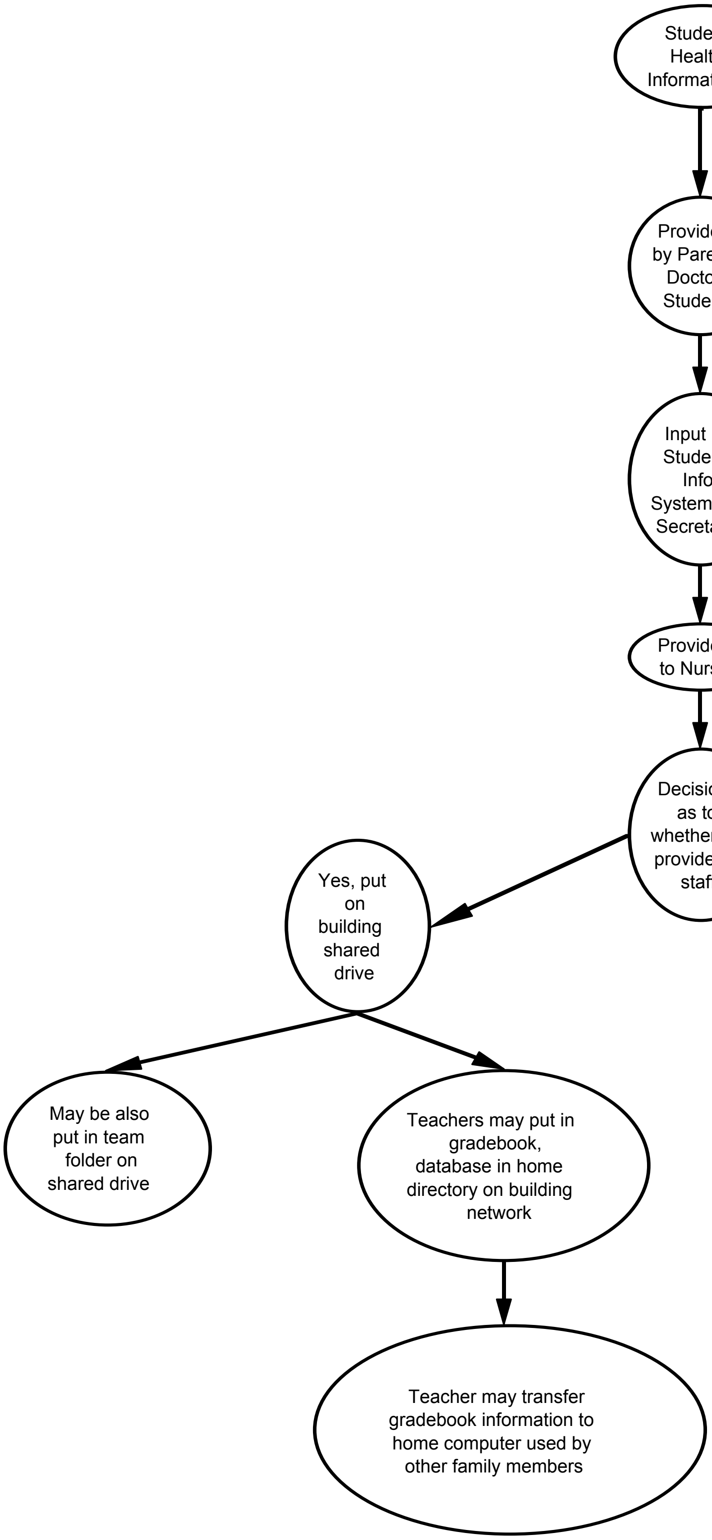
Components—

Characteristics—

Information	***People Who Might Store Information***	***Use of Information***	***Information/Data Storage Options***
Name/Address			
Unlisted Phone Number			
Student Numbers			
SS Number			
Health Info			
Grades			
Homeroom /Schedule			
Free & Reduced Status			
IEP Info			

Information	***People Who Might Store Information***	***Use of Information***	***Information/Data Storage Options***
Attendance			
Emergency Contact Info			
Bus Assignments			
Discipline			
Payroll Info			
Bank Acct Numbers			

Concept Map For Student Health Information


Student Health Information
Provided by Parent/ Doctor/ Student
Input in Student Info System by Secretary
Provided to Nurse
Decision as to whether to provide to staff
Yes, put on building shared drive
No-- remains in SIS
May be also put in team folder on shared drive
Teachers may put in gradebook, database in home directory on building network
Teacher may transfer gradebook information to home computer used by other family members

Sample Privacy Policy for Health Information

Title II. General Principles

All staff members in the Tippecanoe School Corporation receive information on privacy practices at the start of the school year.

Title III. Policy

The Tippecanoe School Corporation collects student health information on each student enrolled in the district. This information includes physician name and phone number, shot records, medications taken, emergency contact information, and any medical conditions which might endanger the student as well as other students and staff, and, any medical conditions which may impact student learning performance.

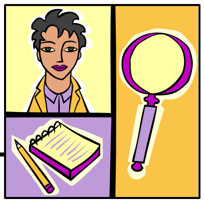
This information is provided by the parent or guardian at registration time and updated as necessary to help assure the accuracy of the information. In addition, physician information may be added to the student's record at any time during the school year. Both emergency contact and physician information is required by the district. If medication is taken during the school day and dispensed by school personnel, medication information is required. Shot records are required by state law.

The information is stored in electronic format in the district student information system. In addition, electronic versions may be stored on the building intranet or in print format in the school office.

If the building principal and school nurse deem that the health information will impact student learning or other school members, the information may be accessed by the student's teachers and staff members who have a need to know.

Electronically maintained information is appropriately secured via password and network settings. Print information is appropriately secured in the school office area.

Privacy Policy Questions



1.0 Information Collection

1.1 What personally identifiable information does School Corporation / district collect?

1.2 Why is the information collected?

1.3 What is the source of the information? Where do we get the information?

1.4 Who within the School Corporation / district collects the information?

1.5 How is the information gathered? What methods are used?

1.6 How is the information kept?

1.7 Who is responsible for the collection of new data sets?

1.8 Who is responsible for ensuring the accuracy of the information received?

1.9 Who is responsible for updating and aging out the information?

1.10 Who is responsible for expunging the information?

1.11 Who is responsible for record retention?

2.0 Information Dissemination and Access

2.1 Who within the School Corporation / district uses the information?

2.2 With who does the school corporation / district share the information?

2.3 Who *has access to the information?*

2.4 Why is it shared?

2.5 How is it shared?

2.6 Who authorizes the sharing or dissemination of the information?

2.7 How do we authenticate users?

3.0 Information Use

3.1 Who within the School Corporation / district controls the information?

3.2 How is it controlled? What systems are used to capture and manage the information?

3.3 For what purpose does the school corporation / district use the information?

3.4 Who, if anyone, has responsibility for determining when the information should be destroyed or aged out?

4.0 Information Maintenance and Retention

4.1 What personally identifiable information is kept?

4.2 How is the information stored—paper or searchable electronic?

4.3 What are the records retention policies?

4.4 Are there policies requiring review for possible purging when new information is available?

4.5 Notification required to those who have accessed information when it is purged?

4.6 Does the school corporation / district have to keep a record of information has been destroyed or purged?

Information	***HD C:/***	***Web Site***	***Network Drive H: District Server/***	***Shared Drives S:/& Collab***	***Flash/Thumb Drive***	***PDA/Palm***	***Portable USB HD***	***Disk/CD/Zip Disk***
Name/Address								
Unlisted Phone Number								
Student Numbers								
SS Number								
Health Info								
Grades								
Homeroom /Schedule								
Free & Reduced Status								
IEP Info								

Information	HD C:/	Web Site	Network Drive H: District Server/	Shared Drives S:/& Collab	Flash/Thumb Drive	PDA/Palm	Portable USB HD	Disk/CD/Zip Disk
Attendance								
Emergency Contact Info								
Bus Assignments								
Discipline								
Payroll Info								
Bank Acct Numbers								

GuidelinesFor Choosing Passwords

A good, strong password should meet all three of these criteria:

1. **Over eight characters** in length. Short passwords are easier to crack than long passwords.

2. **Combines** letters, numbers, and symbols, but:

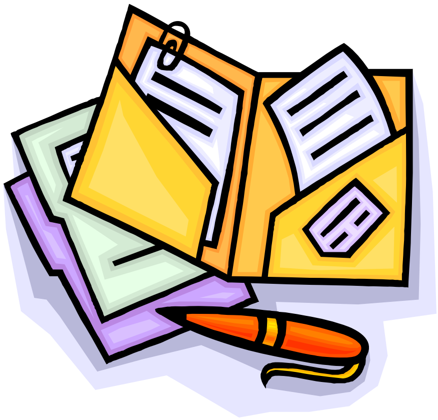
   - **Not sequential** or repeating combinations, such as "12345678," "222222," "abcdefg," or adjacent letters on your keyboard

   - **Not common words with letters replaced** by numbers or symbols, such as “MyL0&1n" or "P@ssw0rd"
     - Unfortunately, hackers know these tricks, too.

3. **Easy for you to remember,** but difficult for others to guess, and:

   - **Not your login name,** your spouse's name, or your birthday.
   -
   - **Not words found in the dictionary,** in any language. Hackers use sophisticated tools that can rapidly guess passwords that are based on words in the dictionary, in a variety of languages, and using words spelled backwards.

   - **Not hard-to-remember.** Random combinations of letters, numbers, and symbols that must be written down to be remembered, can be misplaced, or found by others and used.



Security Options in MS Office

Microsoft Word Documents (Word 2000 and newer)

- Click **File**, then **Save As**
- Click on **Tools** in the upper right corner of the file save dialog box
- Click on **Security Options**
- The Security Options box provides a variety of options:
    - Enter a password in the box next to **Password to open.** (The file will be completely inaccessible without the password)
        - In Word 2002 and 2003, you can click on the **Advanced** button next to the password box to choose a higher level of encryption that is even harder to break
    - Enter a password in the box next to **Password to modify** if it is OK for others to open the file, but you want to restrict who can make changes to the file
- The bottom of the Security Options box also provides some choices to protect the privacy of the document:
    - Remove personal information from file properties on save (creator, etc.)
    - Warn before printing, saving or sending a file that contains tracked changes or comments
    - Store random number to improve merge accuracy
    - Make hidden markup visible when opening or saving
- Click on **OK** to close the Security Options box
- Select a name for your file and click **Save**

Microsoft Excel Documents

- Click on **File**, then **Save As**
- Click on **Tools** in the upper right corner of the file save dialog box
- Click on **General Options**
- Enter a password in the box next to **Password to open** if you wish the file to be completely inaccessible without the password
    - You can click on the **Advanced** button next to the password box to choose a higher level of encryption that is even harder to break into
- Enter a password in the box next to **Password to modify** if it is OK for others to open the file, but you want to restrict who can make changes to the file
- Click on **OK** to close the General Options box
- Select a name for your file and click **Save**

Security Options with Windows

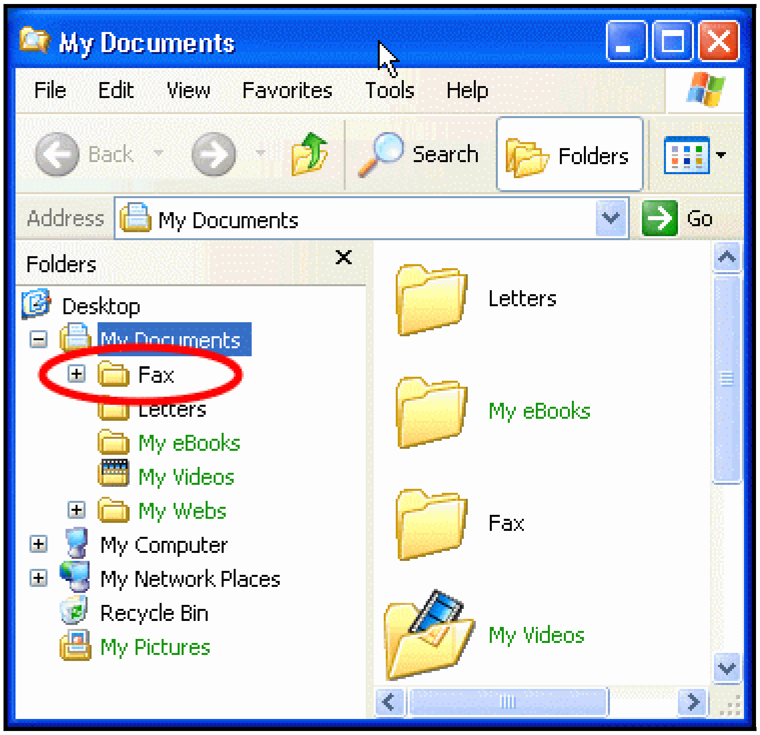
Encrypting

- When files and/or folders are moved, they inherit the permissions of the destination folder.
- When files and/or folders are moved (or copied) to FAT16 or FAT32 file systems, they lose their NTFS permissions because FAT16 and FAT32 volumes do not support NTFS permissions.

Important: Only Windows 2000, Windows XP Pro and Microsoft Windows Server 2003 provide file and folder encryption capabilities.

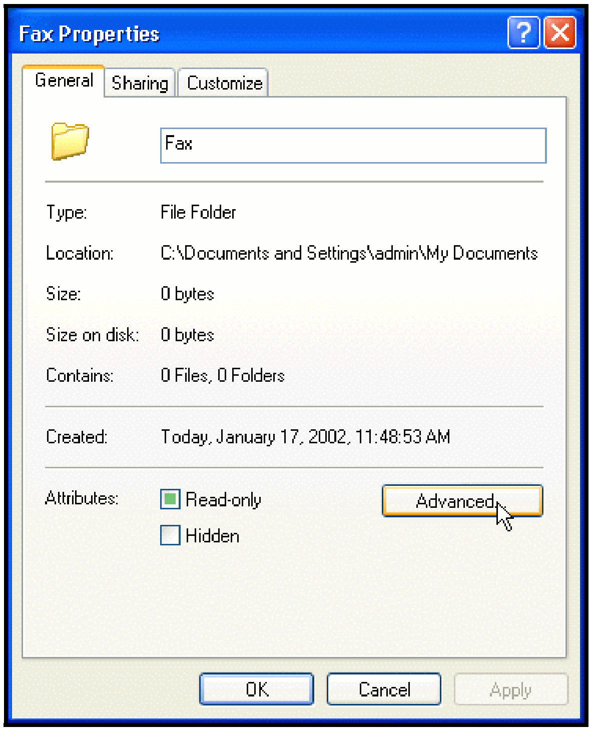
***Note**: Even reinstalling Windows with the same user name or inserting the hard disk into another PC does NOT reveal the data!*

1. Select the folder that you want to encrypt. In our case we want to encrypt our "FAX" folder.



©Center for Education and Research in Information Assurance and Security, Purdue University, 2006

2. Open the FAX folder properties:



Fax Properties

Fax

Type: File Folder

Location: C:\Documents and Settings\admin\My Documents

Size: 0 bytes

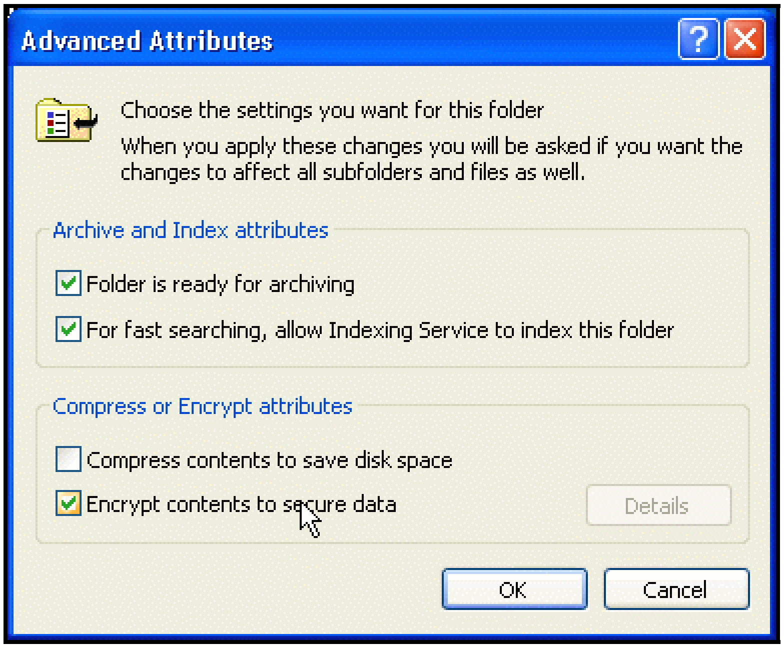
Size on disk: 0 bytes

Contains: 0 Files, 0 Folders

Created: Today, January 17, 2002, 11:48:53 AM

Attributes: ☑ Read-only ☐ Hidden

3. Select the "Encrypt contents..." attribute—Your data is now encrypted!!!!!



Advanced Attributes

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

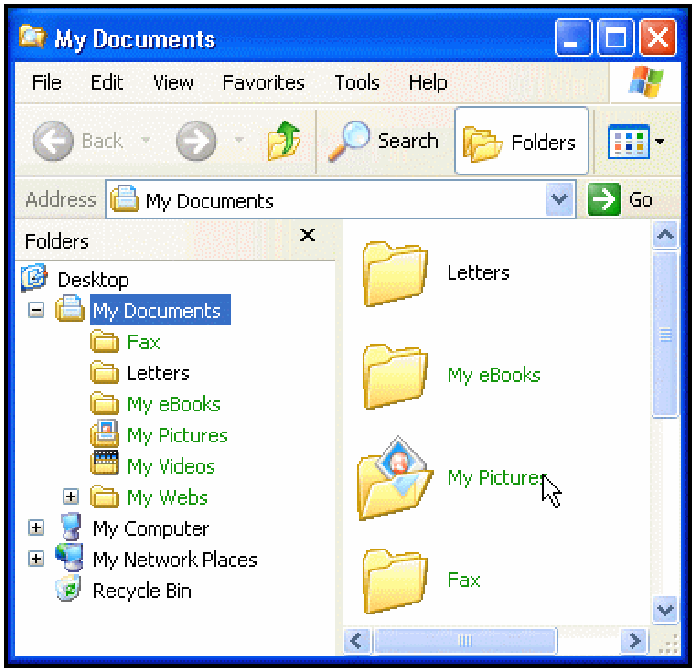
☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

Note: Under Windows XP encrypted folders are displayed with a GREEN color:



Test: Log off and log on as a different user. You will see the file names but you are not able to access them!

Only the following people can decrypt an encrypted file.

- The user who encrypted the file
- Any user who was designated as a recovery agent before the file was encrypted
- Any user who has the public key or private key for the recovery agent or the user that originally encrypted the file
- Any user who has been granted access to the file

NOTE: *You must be the original encrypter of the file/folder or a designated recovery agent for the file to remove the encryption.*

To remove encryption from a file:

1. Use Windows Explorer to browse to the location of the encrypted file that you want to decrypt.
2. Right-click the encrypted file, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. Click to clear the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.

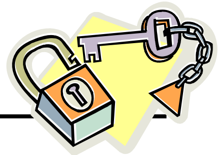
How to Remove Encryption from a Folder

1. Use Windows Explorer to browse to the location of the encrypted folder that you want to decrypt.
2. Right-click the folder, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. Click to clear the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.
5. When you are prompted to confirm the attribute change:
   - If you want to decrypt only the folder, click **Apply the changes to this folder only**, and then click **OK**.
   - If you want to decrypt the folder and its contents, click **Apply changes to this folder, subfolders and files**, and then click **OK**.

Information	***E-Mail Transmission***	***Internet Transmission***	***FTP/Telnet /SSH Transmission***	***Wireless Transmission***	
Name/Address					
Unlisted Phone Number					
Student Numbers					
SS Number					
Health Info					
Grades					
Homeroom /Schedule					
Free & Reduced Status					
IEP Info					

Information	***E-Mail Transmission***	***Internet Transmission***	***FTP/Telnet /SSH Transmission***	***Wireless Transmission***	
Attendance					
Emergency Contact Info					
Bus Assignments					
Discipline					
Payroll Info					
Bank Acct Numbers					

Security Tools Use



	AU	AC	OSE	MSE	TPE	SSL
Transmit an individual file	X			X		
Specify access to a folder on a shared drive		X				
Store a database of records on mobile media (laptop, PDA, flash drive, etc)	X			X	X	
Grades stored on the home directory of a teacher		X	X			
Grades stored on the web based SIS for access by teachers and parents		X				X
Homeroom schedule stored on a portable device (flash drive / PDA)	X			X		
Transfer STN via email to the state	X			X		
Move STN numbers from one building to another	X			X	X	
Store test scores with STN numbers on the hard drive	X	X		X	X	
Report discipline information to the state for required reports via the web						X
Report discipline information to the state for required reports via email	X			X		
Provide transcript information to colleges and other school districts	X			X		
Share IEPs--confidential individualized education plans for special education students via a shared location on a building network, Internet, between school districts						X

- Authentication *(AU)*
- Access control *(AC)*
- Operating system directory/file encryption *(OSE)*
- MS Office encryption *(MSE)*
- Third-party encryption tools *(TPE)*
- Secure Socket Layer *(SSL)*

P3P Example--Shopping With Claudia

Claudia has decided to check out a store called CatalogExample, located at http://www.catalog.example.com/. Let us assume that CatalogExample has placed P3P policies on all their pages, and that Claudia is using a Web browser with P3P built in.

Claudia types the address for CatalogExample into her Web browser. Her browser is able to automatically fetch the P3P policy for that page. The policy states that the only data the site collects on its home page is the data found in standard HTTP access logs. Now Claudia's Web browser checks this policy against the preferences Claudia has given it. Is this policy acceptable to her, or should she be notified? Let's assume that Claudia has told her browser that this is acceptable. In this case, the homepage is displayed normally, with no pop-up messages appearing. Perhaps her browser displays a small icon somewhere along the edge of its window to tell her that a privacy policy was given by the site, and that it matched her preferences.

Next, Claudia clicks on a link to the site's online catalog. The catalog section of the site has some more complex software behind it. This software uses cookies to implement a "shopping cart" feature. Since more information is being gathered in this section of the Web site, the Web server provides a separate P3P policy to cover this section of the site. Again, let's assume that this policy matches Claudia's preferences, so she gets no pop-up messages. Claudia continues and selects a few items she wishes to purchase. Then she proceeds to the checkout page.

The checkout page of CatalogExample requires some additional information: Claudia's name, address, credit card number, and telephone number. Another P3P policy is available that describes the data that is collected here and states that her data will be used only for completing the current transaction, her order.

Claudia's browser examines this P3P policy. Imagine that Claudia has told her browser that she wants to be warned whenever a site asks for her telephone number. In this case, the browser will pop up a message saying that this Web site is asking for her telephone number, and explaining the contents of the P3P statement. Claudia can then decide if this is acceptable to her. If it is acceptable, she can continue with her order; otherwise she can cancel the transaction.

Alternatively, Claudia could have told her browser that she wanted to be warned only if a site is asking for her telephone number and was going to give it to third parties and/or use it for uses other than completing the current transaction. In that case, she would have received no prompts from her browser at all, and she could proceed with completing her order.

Sample P3P Policy

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="forBrowsers"
     discuri="http://www.catalog.example.com/PrivacyPracticeBrowsing.html"
     xml:lang="en">
  <ENTITY>
   <DATA-GROUP>
    <DATA ref="#business.name">CatalogExample</DATA>
    <DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.</DATA>
    <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
    <DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
    <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
    <DATA ref="#business.contact-info.postal.country">USA</DATA>
    <DATA ref="#business.contact-info.online.email">catalog@example.com</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.intcode">1</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.loccode">248</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.number">3926753</DATA>
   </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <DISPUTES-GROUP>
   <DISPUTES resolution-type="independent"
     service="http://www.PrivacySeal.example.org"
     short-description="PrivacySeal.example.org">
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif" alt="PrivacySeal's logo"/>
    <REMEDIES><correct/></REMEDIES>
   </DISPUTES>
  </DISPUTES-GROUP>
  <STATEMENT>
   <PURPOSE><admin/><develop/></PURPOSE>
   <RECIPIENT><ours/></RECIPIENT>
   <RETENTION><stated-purpose/></RETENTION>
   <!-- Note also that the site's human-readable privacy policy MUST mention
             that data is purged every two weeks, or provide a link to this
             information. -->
   <DATA-GROUP>
    <DATA ref="#dynamic.clickstream"/>
    <DATA ref="#dynamic.http"/>
   </DATA-GROUP>
  </STATEMENT>
 </POLICY>
</POLICIES>
```

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

HOME | SEARCH | FAQ | SITE INDEX | CONTACT

search GO

VULNERABILITIES & FIXES | EVALUATIONS & PRACTICES | RESEARCH & ANALYSIS | TRAINING & EDUCATION

Options

Advisories

US-CERT Vulnerability Notes Database

Incident Notes

Current Activity

Related
Tech Tips

AirCERT

Employment Opportunities

more links
CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CSIRT courses

Other Sources of Security Information

Channels

Message

Related Sites

Securing Your Web Browser

Will Dormann and Jason Rafail
CERT Coordination Center

This paper will help you configure your web browser for safer internet surfing. It is written for home computer users, students, small business workers, and any other person who works with limited information technology (IT) support and broadband (cable modem, DSL) or dial-up connectivity. Although the information in this document may be applicable to users with formal IT support as well, organizational IT policies should supersede these recommendations.

I. Why Secure Your Web Browser?

Today, web browsers such as Internet Explorer, Mozilla Firefox, and Safari (to name a few), are installed on almost all computers. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

Ideally, computer users should evaluate the risks from the software they use. Many computers are sold with software already loaded. Whether installed by a computer manufacturer, operating system maker, internet service provider, or by a retail store, the first step in assessing the vulnerability of your computer is to find out what software is installed and how one program will interact with another. Unfortunately, it is not practical for most people to perform this level of analysis.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. In recent months, the CERT/CC has observed a trend whereby new software vulnerabilities are exploited and directed at web browsers through the use of compromised or malicious web sites. This problem is made worse by a number of factors, including the following:

- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer.

- Many web sites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.
- Many users are unaware whether or not their computer has been compromised.
- Many users fail to properly “clean” a compromised computer.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

In addition to following this paper's recommendations, refer to the documentation in the References section for other steps you can take to secure your computer.

II. Understanding Web Browser Features

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. For example, the ActiveX software feature has a history of vulnerabilities that have lead to severe security impacts when enabled.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as email clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser to access web sites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser installed on your computer.

Web sites may require the use of a browser that supports scripting or active content, such as JavaScript or ActiveX controls, or the sites themselves may contain vulnerabilities. Web sites can be considered products, and as a user of the product, you can contact the web site administrators and request that the sites be designed so that they do not require the use of features that may pose a computer security risk.

Some specific web browser features and attributes are described in this document. Understanding what different features do will help you understand how they affect your web browser's functionality and the security of your computer.

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or may download the component from a web site. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

Java is an object-oriented programming language that can be used to develop active content for web sites. A Java Virtual Machine, or JVM, is used to execute the Java code, or “applet,” provided by the web site. The JVM is designed to separate, or “sandbox,” running code so that it does not affect the rest of the system. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets run independently from the operating systems.

Active Content, or plug-ins, are intended for use in the web browser. They are similar to ActiveX controls but cannot be executed outside of a web browser. Macromedia Flash is an example of Active Content that can be provided as a plug-in.

JavaScript is a dynamic scripting language that is used to develop active content for web sites. Unlike Java, JavaScript is a language that is interpreted by the web browser directly. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

VBScript is a programming language that is unique to Microsoft Windows. VBScript is similar to JavaScript, but it is not as widely used in web sites because of its limited compatibility with browsers other than Internet Explorer.

Cookies are text files placed on your computer to store data that is used by a web site. A cookie can contain any information that a web site is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the web site that created them.

Security Zones and the Domain Model are methods Microsoft Windows uses designed to provide multiple levels of security settings for a single system. While primarily used by Internet Explorer, it can be invoked by other applications on the system that use components of Internet Explorer. You can learn more about Microsoft’s Security Zones, the Domain Model, and how to secure them at this web site:

http://www.microsoft.com/windows/ie/using/howto/security/setup.asp.

III. Vulnerabilities and Attack Vectors

Increasingly, attackers are exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and attack other computers. A low-cost way for attackers to gain control of your computer is by exploiting vulnerabilities in web browsers. An attacker can simply create a malicious web page that will install Trojan software or spyware that will steal information from your computer. Additional information about spyware is available in the following document: http://www.cert.org/archive/pdf/spyware2005.pdf. Rather than actively targeting and attacking vulnerable systems, a malicious web site can passively compromise systems as the site is visited. A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

In this section, we will point out some common vulnerabilities in web sites and web browsers that tend to be exploited. We will not go into great detail in this document, but will provide links to other documentation that will help explain the vulnerabilities.

A. ActiveX Controls

ActiveX is a technology that has been plagued with various vulnerabilities and implementation issues. One problem with using ActiveX in a web browser is that it greatly increases the attack surface, or “attackability,” of a system. Vulnerabilities in ActiveX objects may be exploited via Internet Explorer, even if the object was never designed to be used in a web browser. In 2000, the CERT/CC held a workshop to analyze security in ActiveX. The results from that workshop may be viewed here: http://www.cert.org/reports/activeX_report.pdf. Many vulnerabilities associated with ActiveX controls lead to severe impacts. Attackers exploiting ActiveX vulnerabilities can frequently gain control of computers. You can search the US-CERT and CERT/CC web sites for ActiveX vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=activex and http://search.cert.org/query.html?qt=activex.

B. Java

Java is an object-oriented programming language developed by Sun Microsystems. A Java applet is machine-independent and requires a Java Virtual Machine (JVM) on the client computer so that it can execute. Java applets traditionally execute within a “sandbox” where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute. You can search the US-CERT and CERT/CC web sites for Java vulnerabilities at the following URLs:
http://search.us-cert.gov/query.html?qt=java
and http://search.cert.org/query.html?col=certadv&col=vulnotes&qt=java.

C. Cross-Site Scripting

Cross-site scripting, often referred to as CSS or XSS, is a vulnerability in a web site that permits an attacker to leverage the trust relationship that you have with that site. For a high-level description of CSS attacks, please read the whitepaper published at http://www.cert.org/archive/pdf/cross_site_scripting.pdf. Note that cross-site scripting is not usually caused by a failure in the web browser. You can search the CERT/CC web sites for cross-site scripting vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=java and http://search.cert.org/query.html?qt=cross-site+scripting.

D. Cross-Zone and Cross-Domain Vulnerabilities

Most web browsers employ security models to prevent a web site from accessing data in a different domain. These security models are primarily based on the Netscape Same Origin Policy: http://www.mozilla.org/projects/security/components/same-origin.html. Internet Explorer also has a policy to enforce security zone separation: http://msdn.microsoft.com/workshop/security/szone/overview/overview.asp.

Vulnerabilities in these security models can be used to perform actions that a site could not normally perform. The impact can be similar to a cross-site scripting vulnerability. However, if a vulnerability allows for an attacker to cross into the local machine zone or other protected areas, the attacker may be able to execute arbitrary commands on the vulnerable system. You can search the US-CERT and CERT/CC web sites for cross-zone and cross-domain vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=cross-domain and http://search.cert.org/query.html?qt=cross-domain.

E. **Malicious Scripting, Active Content, and HTML**

Some sites may contain malicious scripts, active content, or HTML that will attempt to trick the visitor into providing information, or performing an action that will enable the attacker to gain some privilege. In the absence of vulnerabilities, the attackers rely on social engineering to gain access to the victim's information. However, vulnerabilities in web browsers may be exploited to gain privileges as well. Below is a list of vulnerabilities in web browsers that may provide an exploit vector through the use of malicious code. In 2000, the CERT/CC released a frequently asked questions (FAQ) document on malicious scripting. It is available here: http://www.cert.org/tech_tips/malicious_code_FAQ.html. You can search the US-CERT and CERT/CC web sites for malicious scripting and content vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=malicious+scripting+active+content and http://search.cert.org/query.html?qt=malicious+scripting+active+content.

F. **Spoofing**

As it relates to web browsers, spoofing is a term used to describe methods of faking various parts of the browser user interface. This may include the address or location bar, the status bar, the padlock, or other user interface elements. Phishing attacks often utilize some form of spoofing to help convince the user to provide personal information. If a user's browser is vulnerable to spoofing, they are more likely to fall victim to a phishing attack. You can search the US-CERT and CERT/CC web sites for malicious scripting and content vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=browser+spoof and http://search.cert.org/query.html?qt=browser+spoof. The US-CERT document "Technical Trends in Phishing Attacks" (available at http://www.us-cert.gov/reading_room/phishing_trends0511.pdf) has more information about spoofing and phishing techniques.

IV. How to Secure Your Web Browser

Some software features that provide functionality to a web browser, such as ActiveX, Java, Scripting (JavaScript, VBScript, etc), may also introduce vulnerabilities to the computer system. These may stem from poor implementation of the protocol, poor design, poorly written software, or an insecure configuration. For these reasons, you should understand which browsers support which features and the subsequent risks they could introduce. Some web browsers permit you to fully disable the use of these technologies, while others may only permit you to reduce functionality.

This section shows you how to securely configure a few of the most popular web browsers and how to disable features that can cause vulnerabilities. We encourage you to visit the web site for the browser you use to learn more. If a vendor does not provide documentation on how to secure the browser, we encourage you to contact them and ask for it.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change.

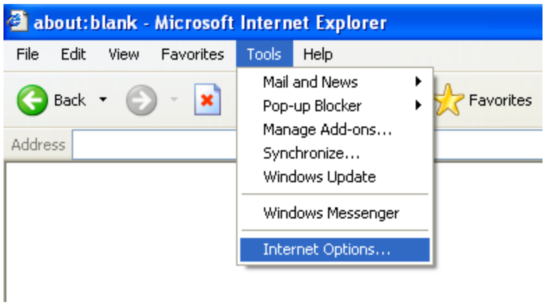
A. Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. Removal of this application is not practical.

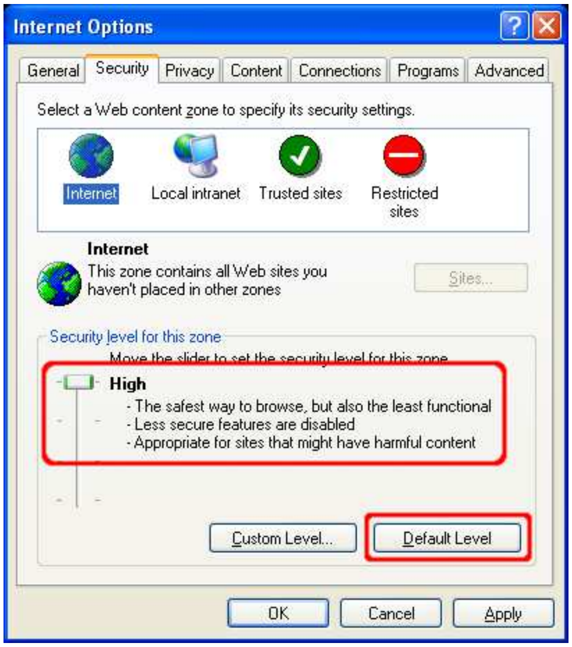
In addition to supporting Java, scripting and other forms of active content, Internet Explorer implements ActiveX technology. While any application is potentially vulnerable to attack, it is possible to mitigate a number of serious vulnerabilities by using a web browser that does not support ActiveX controls. However, using an alternate browser may affect the functionality of some sites that require the use of ActiveX controls. Note that using a different web browser will not remove IE or other Windows components from the system. Other software, such as email clients, may invoke IE, the WebBrowser ActiveX control, or the IE HTML rendering engine (MSHTML). Use of these products may reintroduce the risks presented by these vulnerabilities. Results from the CERT/CC ActiveX workshop in 2000 are available at the following URL: http://www.cert.org/reports/activeX_report.pdf.

Here are steps to disable various features in Internet Explorer. Note that menu options may vary between versions of IE, so you should adapt the steps below as appropriate.

In order to change settings for Internet Explorer, select **Tools** then **Internet Options...**



Select the **Security** tab. On this tab you will find a section at the top, which lists the various security zones that Internet Explorer uses. More information about Internet Explorer security zones is available in the Microsoft document Setting Up Security Zones. For each of these zones, you can select a Custom Level of protection. By clicking the **Custom Level** button, you will see a second window open that permits you to select various security settings for that zone. The **Internet** zone is where all sites initially start out. The security settings for this zone apply to all the web sites that are not listed in the other security zones. We recommend the **High** security setting be applied for this zone. By selecting the High security setting, several features including ActiveX, Active scripting, and Java will be disabled. With these features disabled, the browser will be more secure. Click the **Default Level** button and then drag the slider control up to **High**.



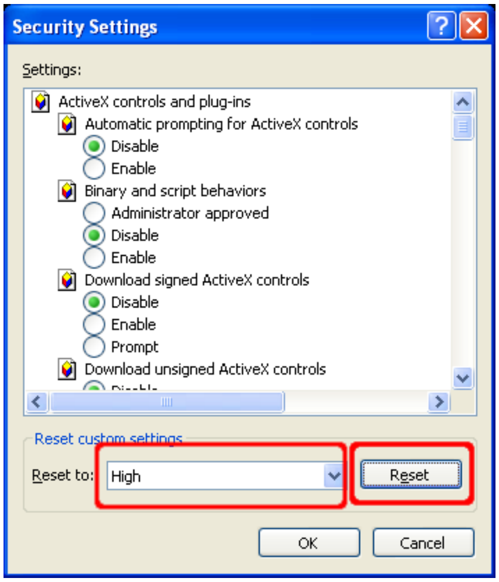
Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

High
- The safest way to browse, but also the least functional
- Less secure features are disabled
- Appropriate for sites that might have harmful content

For a more fine-grained control over what features are allowed in the zone, click the **Custom Level** button. Here you can control the specific security options that apply to the current zone. Default values for the High security setting can be selected by choosing **High** and clicking the **Reset** button to apply the changes.

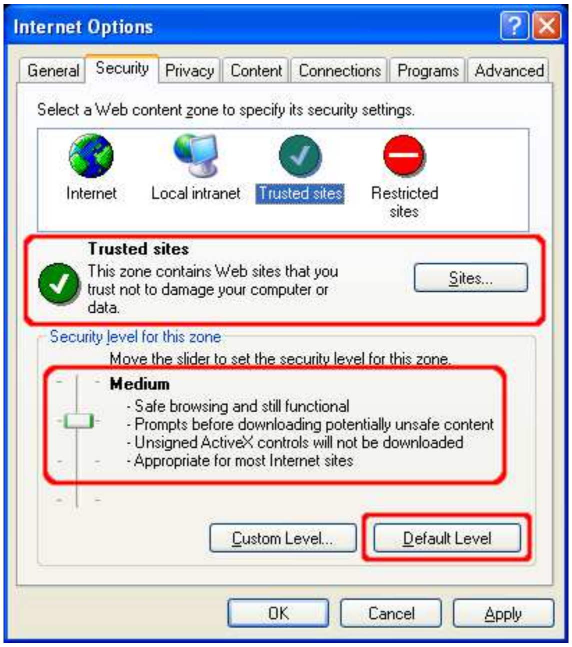


Settings:

ActiveX controls and plug-ins
Automatic prompting for ActiveX controls
● Disable
○ Enable
Binary and script behaviors
○ Administrator approved
● Disable
○ Enable
Download signed ActiveX controls
● Disable
○ Enable
○ Prompt
Download unsigned ActiveX controls

Reset custom settings
Reset to: High

Trusted sites is a security zone for web sites that you believe are securely designed and contain trustworthy content. To add or remove sites from this zone, you can click the **Sites...** button. This will open a new window that will list the sites that you trust and permit you to add or remove sites. You may also require that only sites with Secure Sockets Layer (SSL) implemented can be active in this zone. This permits you to verify that the site you are visiting is the site that it claims to be.

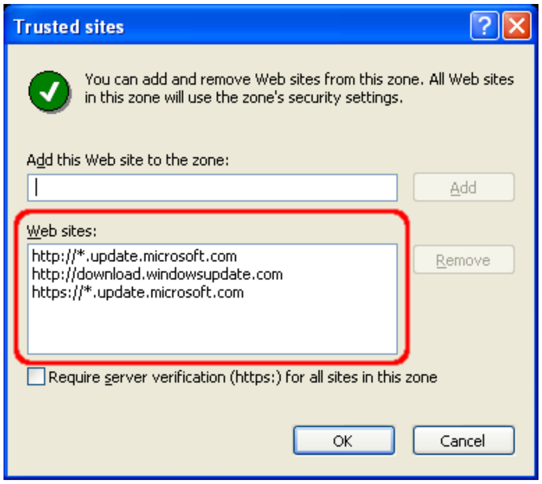


Select a Web content zone to specify its security settings.

Trusted sites
This zone contains Web sites that you trust not to damage your computer or data.

Security level for this zone
Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites



You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

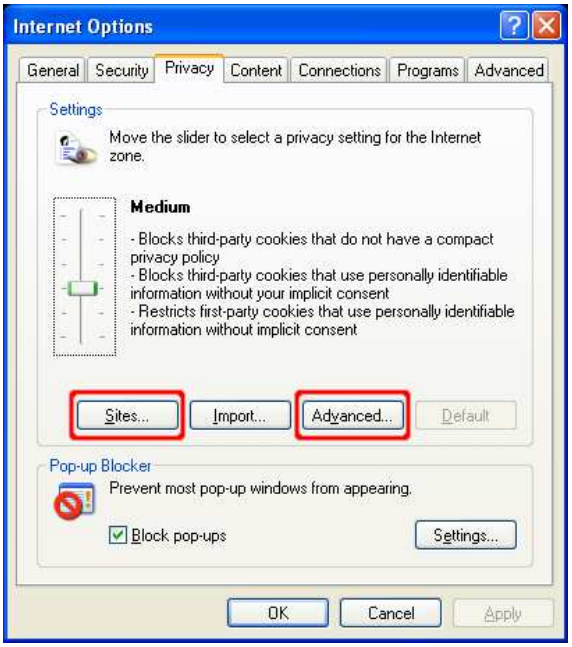
Add this Web site to the zone:

Web sites:
http://*.update.microsoft.com
http://download.windowsupdate.com
https://*.update.microsoft.com

□ Require server verification (https:) for all sites in this zone

We recommend setting the security level for the **Trusted sites** zone to **Medium**. When the Internet Zone is set to **High**, you may encounter web sites that do not function properly due to one or more of the associated security settings. This is where the **Trusted sites** zone can help. If you trust that the site will not contain malicious code, you can add it to the list of sites in the Trusted sites zone. Once a site is added to this zone, features such as ActiveX and active scripting will be enabled. The benefit of this type of configuration is that IE will be more secure by default, and sites can be "whitelisted" in the Trusted sites zone to gain extra functionality.

The **Privacy** tab contains settings for cookies. Cookies are text files placed on your computer by various sites that you visit either directly (first-party) or indirectly (third-party) through ad banners, for example. A cookie can contain any data that a site wishes to store. It is often used to track your computer as you move through a web site and store information such as preferences or credentials. We recommend that you select the **Advanced** button and select **Override automatic cookie handling**. Then select **Prompt** for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your computer. You can then evaluate the originating site, whether you wish to accept or deny the cookie, and what action to take in the future (always accept, always block, or continue to ask).



Internet Options

Settings

Move the slider to select a privacy setting for the Internet zone.

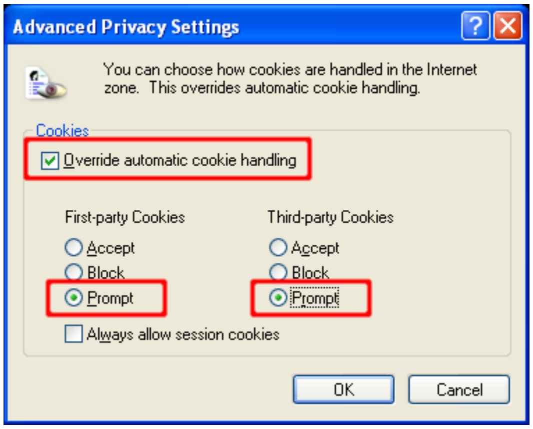
Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Block pop-ups



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

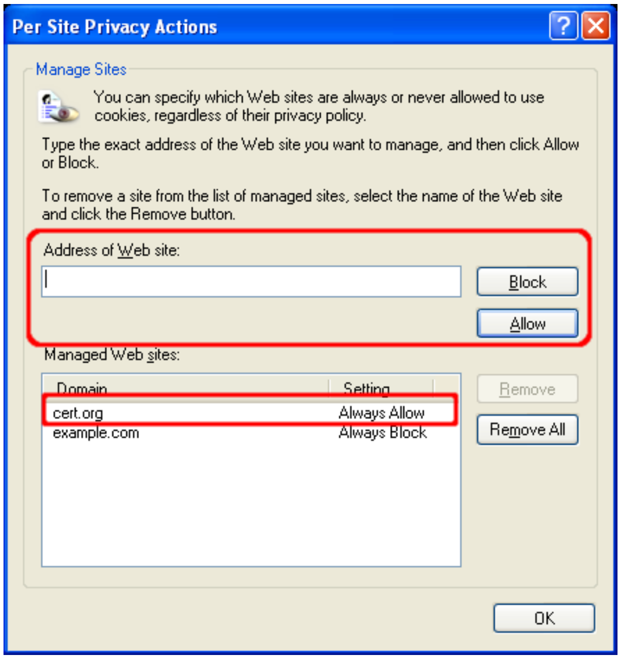
Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
○ Accept	○ Accept
○ Block	○ Block
● Prompt	● Prompt

□ Always allow session cookies

By selecting the **Sites...** button, you can manage the cookie settings for specific sites. You can add or remove sites, and you can change the current settings for existing sites. The bottom section of this window will specify the domain of the site and the action to take when that site wants to place a cookie on your computer. You can use the upper section of this window to change these settings.



Per Site Privacy Actions

Manage Sites

You can specify which Web sites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the Web site you want to manage, and then click Allow or Block.

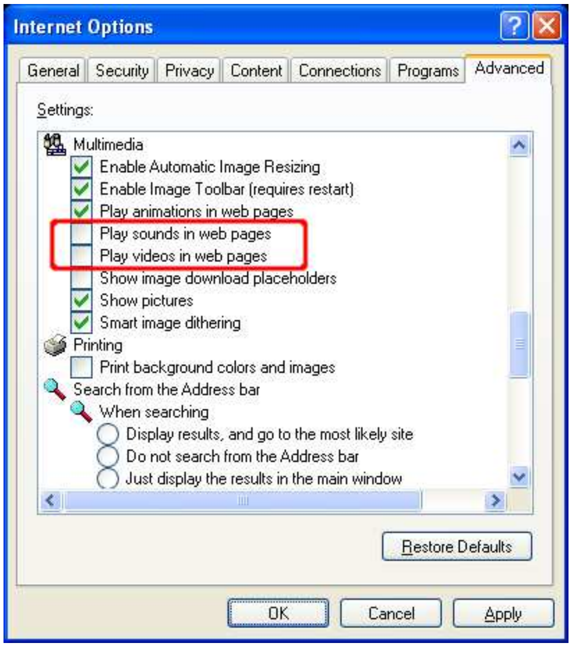
To remove a site from the list of managed sites, select the name of the Web site and click the Remove button.

Address of Web site:

Managed Web sites:

Domain	Setting
cert.org	Always Allow
example.com	Always Block

The **Advanced** tab contains settings used by all zones. The settings contained in the **Multimedia** section have features that you can adjust to protect against some potential vulnerabilities. For instance, attackers may be able to track your usage or exploit the software you use to play multimedia data. We recommend disabling the options to play sounds and videos:



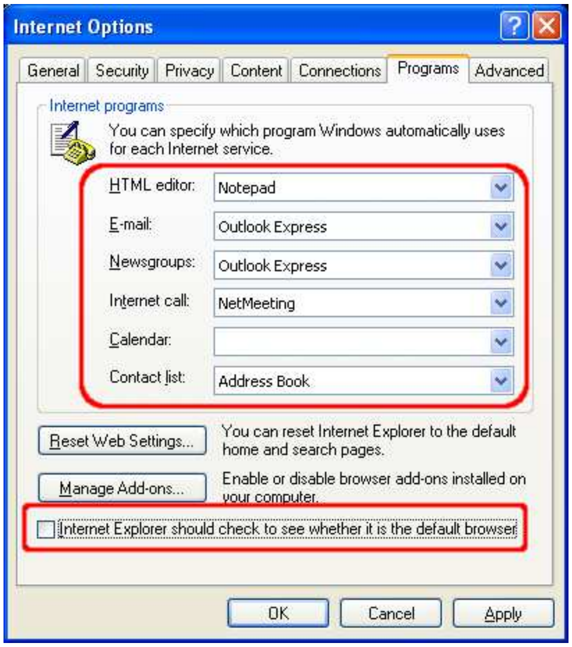
Settings:

Multimedia
- ☑ Enable Automatic Image Resizing
- ☑ Enable Image Toolbar (requires restart)
- ☑ Play animations in web pages
- □ Play sounds in web pages
- □ Play videos in web pages
- □ Show image download placeholders
- ☑ Show pictures
- ☑ Smart image dithering

Printing
- □ Print background colors and images

Search from the Address bar
- When searching
  - ○ Display results, and go to the most likely site
  - ○ Do not search from the Address bar
  - ○ Just display the results in the main window

Under the **Programs** tab, you can specify your default applications for viewing web sites, email messages, and other network related tasks. You can also prevent Internet Explorer from showing you a message asking to be your default web browser.



Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor: Notepad

E-mail: Outlook Express

Newsgroups: Outlook Express

Internet call: NetMeeting

Calendar:

Contact list: Address Book

You can reset Internet Explorer to the default home and search pages.

Enable or disable browser add-ons installed on your computer.

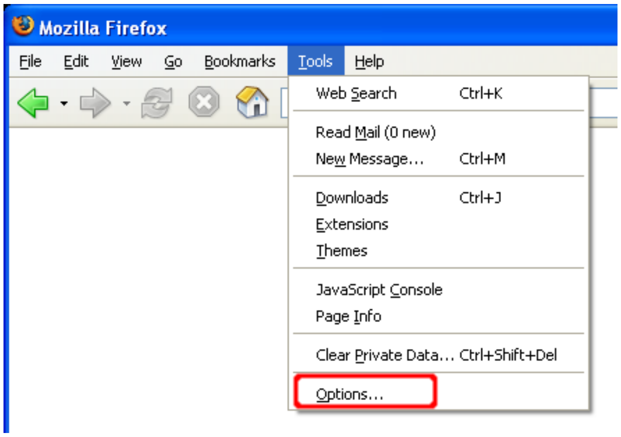
□ Internet Explorer should check to see whether it is the default browser

B. Mozilla Firefox

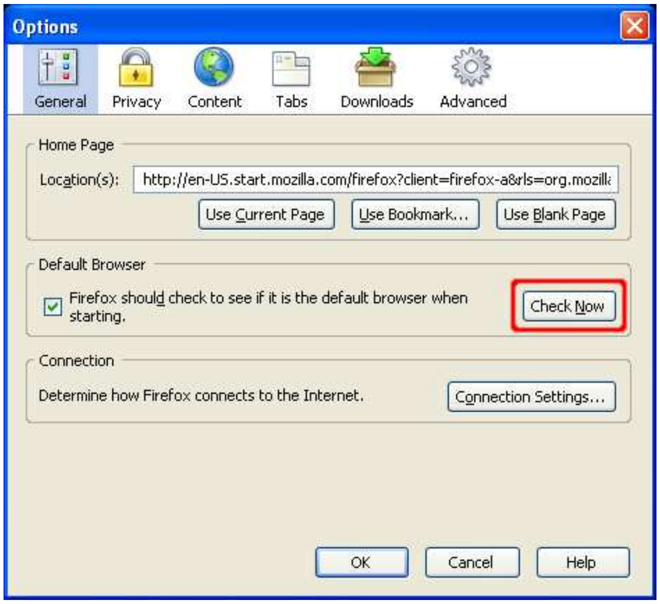
Mozilla Firefox supports many of the same features as Internet Explorer, with the exception of ActiveX and the Security Zone model. We recommend looking in the **Help**, **For Internet Explorer Users** menu to understand the different terminology used by the two browsers.

Following are steps to disable various features in Mozilla Firefox. Note that some menu options may change between versions or may appear in different locations depending on the host operating system. You should adapt the steps below as appropriate.

To edit the settings for Mozilla Firefox, select **Tools**, then **Options**.



You will then see an Options window that has a row of categories along the top. The first category of interest is the **General** category. Under this section, for instance, you can set Firefox as your default browser.

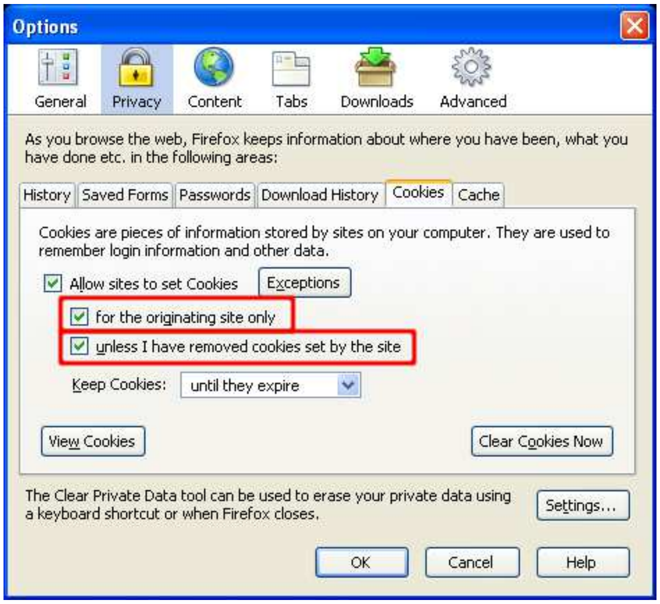


Location(s): http://en-US.start.mozilla.com/firefox?client=firefox-a&rls=org.mozill

☑ Firefox should check to see if it is the default browser when starting.

Determine how Firefox connects to the Internet.

Under the Privacy category, you can select the Cookies subcategory. Here you can disable cookies or change your preferences for how the browser handles them. In general, we recommend enabling cookies **for the original site only**. Additionally, by enabling the option **unless I have removed cookies set by the site**, a web site can be “blacklisted” from setting cookies when its cookies are removed manually.



As you browse the web, Firefox keeps information about where you have been, what you have done etc. in the following areas:

Cookies are pieces of information stored by sites on your computer. They are used to remember login information and other data.

☑ Allow sites to set Cookies

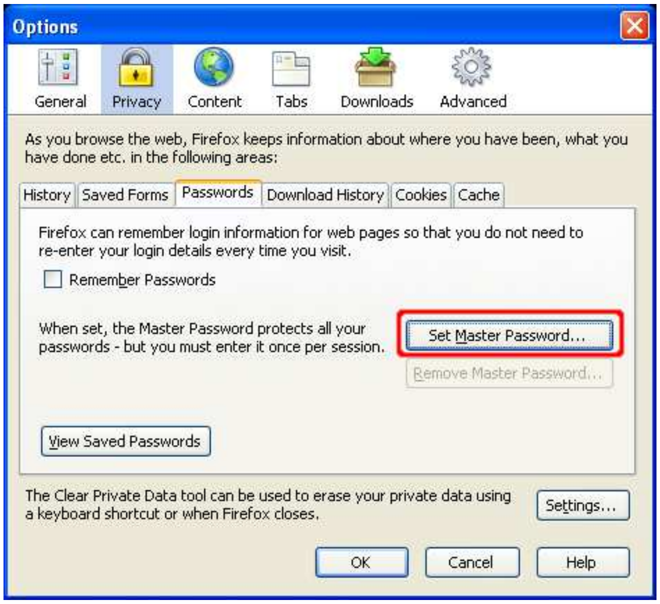
☑ for the originating site only

☑ unless I have removed cookies set by the site

Keep Cookies: until they expire

The Clear Private Data tool can be used to erase your private data using a keyboard shortcut or when Firefox closes.

Many web browsers will allow you to store login information. In general, we recommend against using such features. Should you decide to use the feature, ensure that you use the measures available to protect the password data on your computer. Under the **Privacy** category, the **Passwords** subcategory contains various options to manage stored passwords, and a **Master Password** feature to encrypt the data on your system. We encourage you to use this option if you decide to let Mozilla Firefox manage your passwords.



As you browse the web, Firefox keeps information about where you have been, what you have done etc. in the following areas:

Firefox can remember login information for web pages so that you do not need to re-enter your login details every time you visit.

☐ Remember Passwords

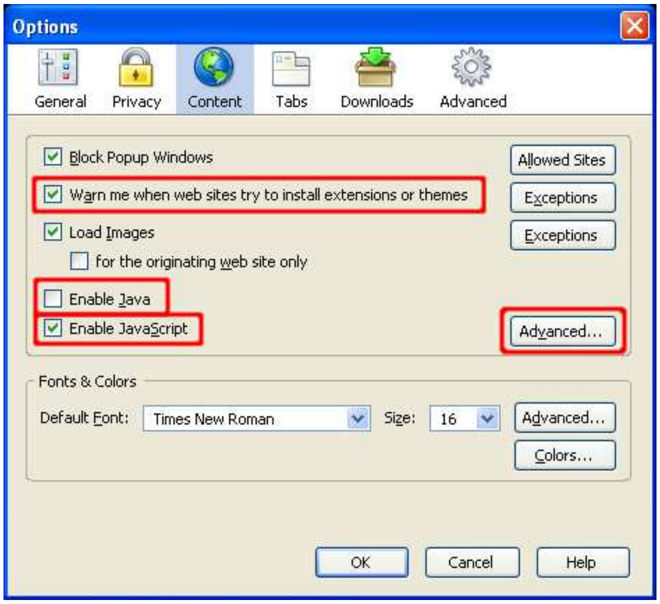
When set, the Master Password protects all your passwords - but you must enter it once per session.

The Clear Private Data tool can be used to erase your private data using a keyboard shortcut or when Firefox closes.

The **Content** category has an option to **Enable Java**. Java is a programming language that permits web site designers to run applications on your computer. We recommend disabling this feature unless required by the site you wish to visit. Again, you should determine if this site is trustworthy and whether you want to enable Java to view the site's content. After you are finished visiting the site, we recommend disabling Java until you need it again.

The **Warn me when web sites try to install extensions or themes** option will display a warning bar at the top of the browser when a web site attempts to take such an action.

Press the **Advanced** button to disable specific JavaScript features. We recommend disabling all of the options displayed in this dialog.



☑ Block Popup Windows

☑ Warn me when web sites try to install extensions or themes

☑ Load Images

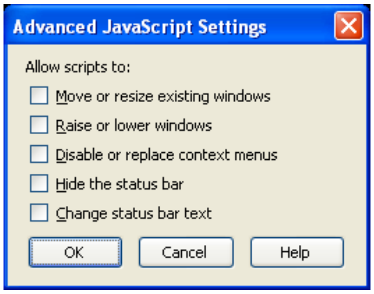
□ for the originating web site only

□ Enable Java

☑ Enable JavaScript

Fonts & Colors

Default Font: Times New Roman Size: 16



Allow scripts to:

□ Move or resize existing windows

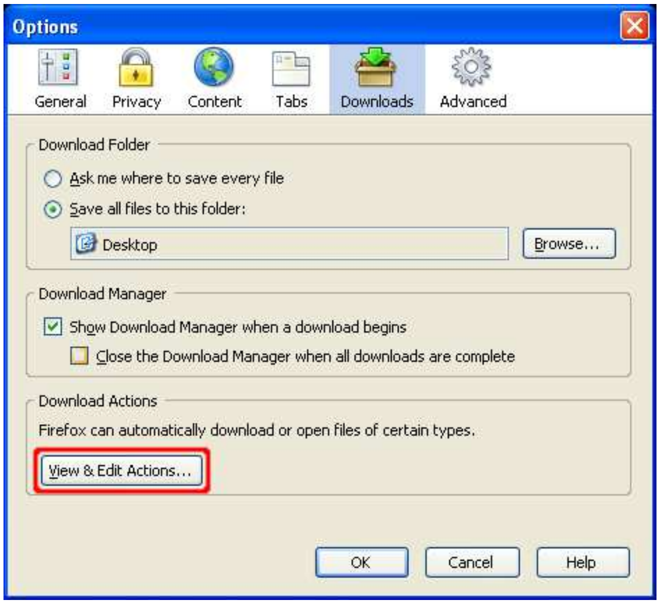
□ Raise or lower windows

□ Disable or replace context menus

□ Hide the status bar

□ Change status bar text

The **Downloads** section has an option to modify actions taken when files are downloading. Any time a file type is configured to open automatically with an associated application, this can make the browser more dangerous to use. Vulnerabilities in these associated applications can be exploited more easily when they are configured to open automatically. Click the **View & Edit Actions** button to view the current download settings and modify them if necessary.



Download Folder

○ Ask me where to save every file

● Save all files to this folder:

Desktop

Download Manager

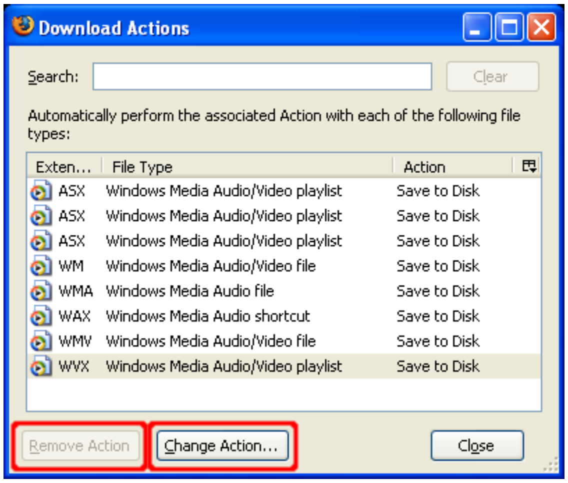
☑ Show Download Manager when a download begins

□ Close the Download Manager when all downloads are complete

Download Actions

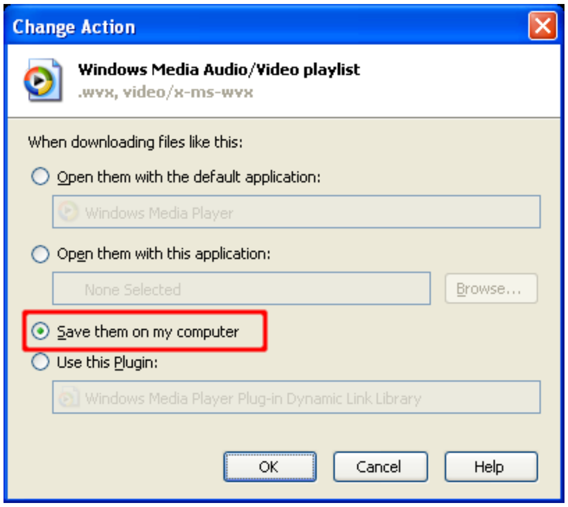
Firefox can automatically download or open files of certain types.

The Download Actions dialog shows the file types and the actions the browser will perform when it encounters a given file type. For any file type listed, click on either **Remove Action** or **Change Action...**. If you click on **Change Action...**, select **Save them on my computer** to save files of that type to the computer. This helps prevent automated exploitation of vulnerabilities that may exist in these applications.



Automatically perform the associated Action with each of the following file types:

Exten...	File Type	Action
ASX	Windows Media Audio/Video playlist	Save to Disk
ASX	Windows Media Audio/Video playlist	Save to Disk
ASX	Windows Media Audio/Video playlist	Save to Disk
WM	Windows Media Audio/Video file	Save to Disk
WMA	Windows Media Audio file	Save to Disk
WAX	Windows Media Audio shortcut	Save to Disk
WMV	Windows Media Audio/Video file	Save to Disk
WVX	Windows Media Audio/Video playlist	Save to Disk



Windows Media Audio/Video playlist
.wvx, video/x-ms-wvx

When downloading files like this:

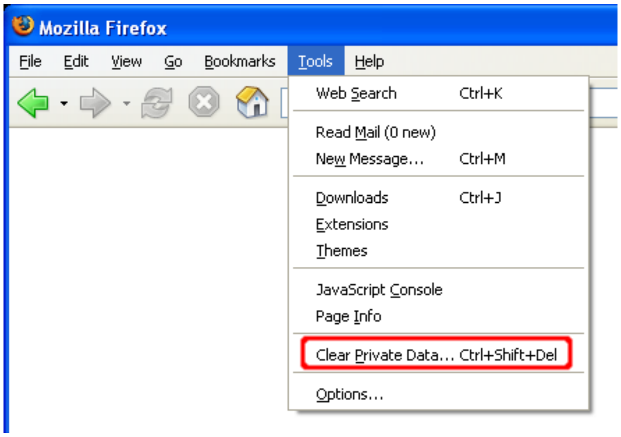
○ Open them with the default application:
Windows Media Player

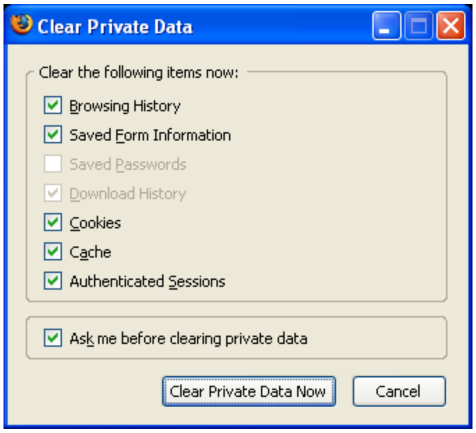
○ Open them with this application:
None Selected

● Save them on my computer

○ Use this Plugin:
Windows Media Player Plug-in Dynamic Link Library

Firefox 1.5 includes a feature to **Clear Private Data**. This option will remove potentially sensitive information from the web browser. Select **Clear Private Data...** from the **Tools** menu to use this privacy feature.





Clear the following items now:

☑ Browsing History
☑ Saved Form Information
□ Saved Passwords
☑ Download History
☑ Cookies
☑ Cache
☑ Authenticated Sessions

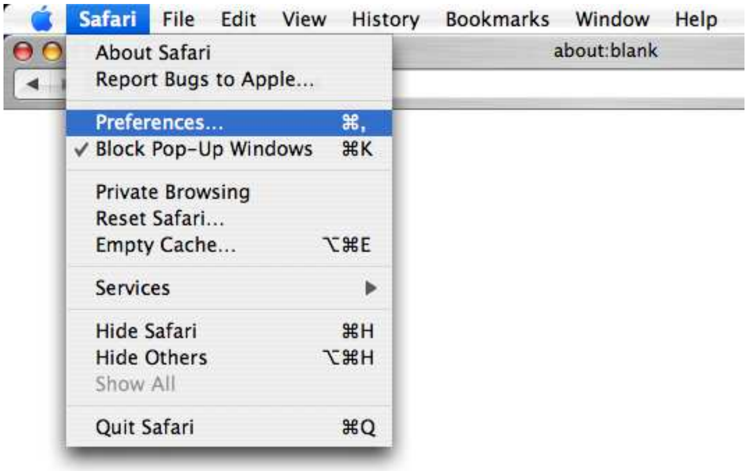
☑ Ask me before clearing private data

C. Apple Computer's Safari web browser

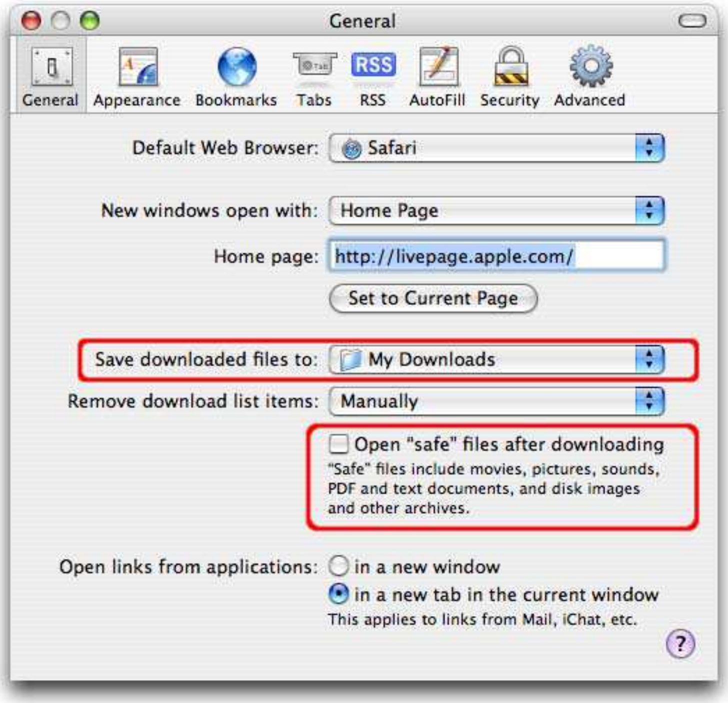
Safari supports many of the same features as Mozilla Firefox. This section describes steps to disable various features in Safari. Note that some menu options may change over time, and you should adapt the steps below as appropriate.

In order to change settings, select **Safari** and then select **Preferences...**

Note that on the Safari menu, you can also select the option “Block Pop-up Windows”. This option will prevent sites from opening another window through the use of scripting, or active content. Be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.



Once you select the **Preferences** menu, the window depicted below will open. The first tab to examine is the **General** tab. On this tab, you can set up many options such as **Save downloaded files to:** and **Open “safe” files after downloading**. We recommend that you save downloaded files to a temporary folder that you create for downloading files. We also recommend that you deselect the **Open “safe” files after downloading** option.



Default Web Browser: Safari

New windows open with: Home Page

Home page: http://livepage.apple.com/

Set to Current Page

Save downloaded files to: My Downloads

Remove download list items: Manually

□ Open "safe" files after downloading

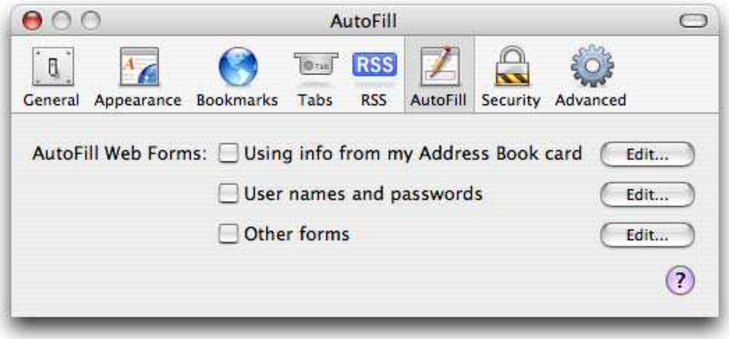
"Safe" files include movies, pictures, sounds, PDF and text documents, and disk images and other archives.

Open links from applications: ○ in a new window

● in a new tab in the current window

This applies to links from Mail, iChat, etc.

The next section of interest is the **AutoFill** tab. On this tab, you can select what types of forms your browser will fill in automatically. In general, we recommend against using AutoFill features. If someone can gain access to your computer, or to the data files, then the AutoFill feature may permit them even easier access to other sites that they would not otherwise have the ability to access. However, if used with appropriate protective measures, it may be acceptable to enable AutoFill. We recommend using filesystem encryption software such as OS X FileVault to provide additional security for files that reside in a user's home directory.



AutoFill Web Forms: □ Using info from my Address Book card Edit...

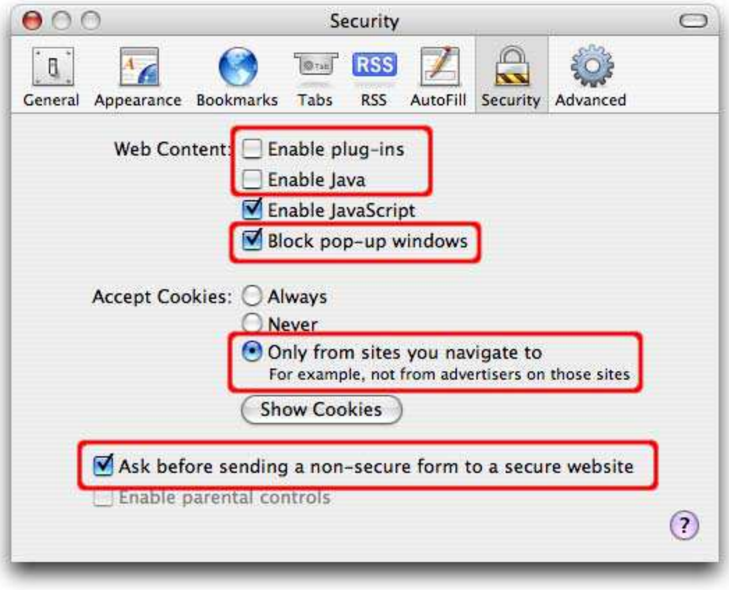
□ User names and passwords Edit...

□ Other forms Edit...

The **Security** tab provides several options. The **Web Content** section permits you to enable or disable various forms of scripting and active content. We recommend disabling the first three options in this section, and only enabling them when you require the functionality of these features. We recommend selecting the **Block Pop-up Windows** option. Remember that this option will prevent sites from opening another window through the use of scripting, or active content. Again, be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.

It is safer to use Safari without plug-ins and Java, so we recommend disabling the options **Enable plug-ins** and **Enable Java**. It is also safer to disable JavaScript. However, many web sites require JavaScript for proper operation.

In this dialog you can disable cookies and can also view or remove cookies that have been set. In general, we recommend disabling cookies and enabling them only when you visit a site that requires their use. At this point, you should determine if the site is trustworthy (i.e., contains no malicious content and is securely designed) and determine whether you want to allow cookies to access the site's content. After you are finished visiting the site, we recommend disabling cookies until you need to access a site that requires cookies. You can limit cookies to the sites that you navigate to by selecting the option **Only from sites you navigate to**. This will permit sites that you visit to set cookies, but not third-party sites. Finally, we recommend selecting the **Ask before sending a non-secure form to a secure website** option. This will alert you when data is sent to a secure web site over an insecure channel.



Web Content: □ Enable plug-ins

□ Enable Java

☑ Enable JavaScript

☑ Block pop-up windows

Accept Cookies: ○ Always

○ Never

● Only from sites you navigate to
For example, not from advertisers on those sites

☑ Ask before sending a non-secure form to a secure website

□ Enable parental controls

D. Other Browsers

Other web browsers may have similar options to those described in the previous sections. Please refer to the browser documentation to determine which options are available and how to make the necessary changes. For example, here are some other popular browsers:

Mozilla Suite - http://www.mozilla.org/products/mozilla1.x

Opera - http://www.opera.com/support/tutorials/security
Konqueror - http://www.konqueror.org
Netscape - http://browser.netscape.com

V. Keeping Your Computer Secure

In addition to selecting and securing your web browser, you can take other steps to protect your computer:

A. **Read the CERT/CC Home Network Security and Home Computer Security documents.**

B. **Install and use antivirus software**

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available. A partial list of antivirus vendors is available on the CERT/CC web site.

C. **Enable automatic software updates if available**

Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation tells you how to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered, you may need to check the vendor's web site periodically for updates.

D. **Avoid unsafe behavior**

Additional information on this topic can be found in the document Home Network Security.

- Use caution when opening email attachments or when using peer-to-peer file sharing, instant messaging, or chat rooms.
- Don't enable file sharing on network interfaces exposed directly to the internet.

E. **Follow the principle of least privilege — don't enable it if you don't need it**

Consider creating and using an account with limited privileges instead of an “administrator” or “root” level account for everyday tasks. Depending on the operating system, you only need to use administrator-level access when installing new software, changing system configurations, and other important tasks. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far more risky to be logged in as an administrator all the time.

References

US-CERT References

- Avoiding Social Engineering — http://www.us-cert.gov/cas/tips/ST04-014.html
- Browsing Safely: Understanding Active Content and Cookies — http://www.us-cert.gov/cas/tips/ST04-012.html
- Evaluating Your Web Browser's Security Settings — http://www.us-cert.gov/cas/tips/ST05-001.html
- Spyware — http://www.us-cert.gov/reading_room/spyware.pdf
- Understanding Internationalized Domain Names — http://www.us-cert.gov/cas/tips/ST05-016.html
- Understanding Web Site Certificates — http://www.us-cert.gov/cas/tips/ST05-010.html
- Understanding Your Computer: Web Browsers — http://www.us-cert.gov/cas/tips/ST04-022.html

CERT/CC References

- Before You Connect a New Computer to the Internet — http://www.cert.org/tech_tips/before_you_plug_in.html
- Home Computer Security — http://www.cert.org/homeusers/HomeComputerSecurity/
- Home Network Security — http://www.cert.org/tech_tips/home_networks.html
- Technical Trends in Phishing Attacks — http://www.cert.org/archive/pdf/Phishing_trends.pdf

Microsoft Windows XP References

- Improve the safety of your browsing and e-mail activities — http://www.microsoft.com/athome/security/online/browsing_safety.mspx
- Microsoft Windows XP Baseline Security Checklist — http://www.microsoft.com/technet/archive/security/chklist/xpcl.mspx
- Microsoft Windows XP Service Pack 2 — http://www.microsoft.com/windowsxp/sp2/default.mspx
- Microsoft's Protect Your PC — http://www.microsoft.com/protect/
- Setting Up Security Zones — http://www.microsoft.com/windows/ie/using/howto/security/setup.mspx
- Using the Internet Connection Firewall — http://www.microsoft.com/windowsxp/home/using/howto/homenet/icf.asp

Apple Macintosh OSX References

- Apple Product Security — http://www.apple.com/support/security/
- Apple Security Updates — http://docs.info.apple.com/article.html?artnum=61798
- How to Keep Network Computers Secure — http://docs.info.apple.com/article.html?artnum=61534
- OSX Security Features Overview — http://www.apple.com/macosx/features/security/

Linux References

- Debian Security Information — http://www.debian.org/security/
- Gentoo Security Handbook — http://www.gentoo.org/doc/en/security/
- Mandriva Security Advisories — http://www.mandriva.com/security/advisories
- RedHat Security and Errata — http://www.redhat.com/apps/support/errata/
- Slackware Security Advisories — http://www.slackware.com/security/
- SUSE Security (US/Canada) — http://www.novell.com/linux/security/securitysupport.html
- Ubuntu Security notices — http://www.ubuntu.com/usn/

System Administrator References

- Description of Internet Explorer security zones registry entries — http://support.microsoft.com/?kbid=182569
- How To Set Advanced Settings In Internet Explorer by Using Group Policy Objects — http://support.microsoft.com/?kbid=274846
- Internet Explorer Administration Kit — http://www.microsoft.com/technet/prodtechnol/ie/ieak

Revision History

January 23, 2006	Inital Release

Hot Tips