Privacy and Security

Computer Literacy

Privacy in Cyberspace

- Privacy: an individual's ability to restrict or eliminate the collection, use, and sale of confidential personal information
 - Definition and concern depends upon individual
 - Westin survey for Equifax found 3 categories of people
 - Fundamentalist: highly concerned
 - Pragmatist: moderately concerned
 - Unconcerned: low level of concern
- The problem is collection of information without consent
- Anonymity: the ability to communicate without disclosing one's identity
 - More difficult with the use of computers and the Internet

Technologies that jeopardize anonymity

- Cookies
- Global unique identifiers
- Ubiquitous computing
- Radio frequency identification

Cookies

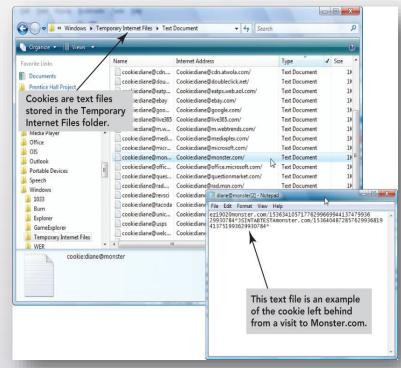
Small text files written to your hard disk by web sites visited

Intent: store data about you and your preferences so it doesn't have

to keep asking

Examples include:

- Name, address, password, credit card
- Items in a shopping cart
- Track your browsing habits
- Gather personal information without your consent
- Can be disabled
- Banner ads
 - targeted display ads based on cookies



Global unique identifier (GUID)

Identification number produced by software or a piece of hardware

- Web servers read the GUID
- Users are not always aware of the GUID
- If used, companies typically allow users to opt out
- Civil liberties groups and public concern have decreased the use of GUIDs

Ubiquitous computing

The concept that computing appears anytime everywhere (everyware)

- Interacting with multiple networked devices
- Smart things allow for ubiquitous data collection and tracking
- Examples:
 - Active badge transmits infrared signals to create an electronic trail
 - Location data in cell phones
 - Health data in wearable devices
 - Search history and always-on-microphone on home assistants

Radio frequency identification (RFID)

Automatically identify and track objects using radio waves

- Used for tracking and inventory control in stores
- Embedded in passports
- Recognizes microchips in pets
- Research on embedding chips in humans



Protecting privacy at home

- Create logins and passwords for each person using the computer
- Do not save account numbers or passwords written down
- Use strong passwords



Do use:

- Difficult to guess passwords
- At least 16 characters or more
- Uppercase, lowercase, numbers, and special characters



Do not use:

- Recognizable word or phrase
- Name of anything/anyone close to you
- Recognizable strings of numbers (SSN, birthdates, etc.)

Protecting privacy at work

- Employee monitoring
 - Majority of large U.S. employers observe employee phone calls, e-mails, Web browsing habits, and computer files
- Refrain from making personal calls on a work phone
- Avoid using company e-mail for personal purposes
- Assume you are monitored
- Be aware of shoulder surfing

Are social networking sites spying on you?



Monitored activity

- Things we do
- Information we provide
 - Address, school, location, preferences
 - Images
 - Video
 - Day-to-day activity
 - Holidays
- Network and connections
- Any payments
- Device information
- What happens to collected data if your account is deleted?

How does social media use this information?

- Marketing
- Studies and experiments
- Personal information sold to advertisers
- Other actors
 - Hotels
 - Standardized testing companies
 - Insurance companies
 - Landlords
 - Universities
 - Potential employers
 - Police

Security



Computer security risk

An event or action that could cause damage to a computer system or its data

- Wireless LAN security options include:
 - WEP (Wired Equivalent Privacy)
 - First security standard
 - Easily hacked
 - WPA (Wi-Fi Protected Access)
 - Interim standard to address major WEP flaws
 - Only use this if WPA2 is not available
 - WPA2
 - Current standard
 - Most secure wireless standard available
- Vacation hacking: tricking travelers into using phony WiFi hot spots known as evil twins

Computer security threats

- Social engineering
- Malware
- Corporate espionage
- Pod slurping
- Backdoors
- Information warfare
- Attacks on safety-critical systems
- Cyberterrorism

Protecting your computer

- Firewalls
- Antivirus
- Antispyware
- Use secure passwords
- Limit physical access to devices
- Biometric authentication
- Only connect to trusted/secure WiFi
- Be conscious of social engineering