UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 4: Malware and Social Engineering Attacks

Objectives

- Describe the differences between a virus and a worm
- List the types of malware that conceals its appearance
- Identify different kinds of malware that is designed for profit
- Describe the types of social engineering psychological attacks
- Explain physical social engineering attacks

What is Malware?

MALWARE

Combination of the words **malicious** and **software** and is used to describe, in general terms, any type of **'bad' code** we may find **in computer**

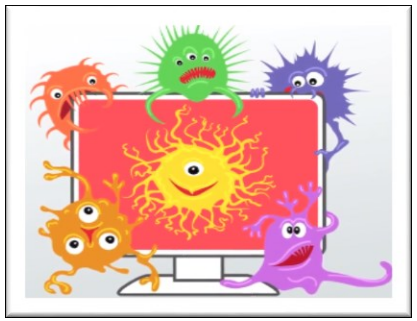
What is Malware?

- Enters a computer system without the owner's knowledge or consent
- Malware can infect computers and devices in several ways and comes in a number of forms, just a few of which include viruses, worms, Trojans, spyware and more

- Primary objectives of malware
- Infecting systems
- Concealing its purpose
- Making profit

Malware that spread : Computer Virus

A piece of software that can be attached to another program or file
- The program or file is set to be the 'host'

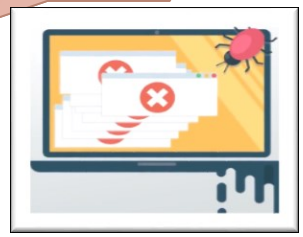


Virus cannot automatically spread to another computer
Relies on user action to spread

Examples of virus actions
–Cause a computer to repeatedly crash
–Erase files from or reformat hard drive
–Turn off computer's security settings

Computer virus may attach itself to files that download and install to computer

Virus spread when the infected files is pass from system to system



Malware that spread : Computer Virus

Virus Infection Methods

Appender Infection

- Virus appends itself to end of a file
- Moves first three bytes of original file to virus code
- Replaces them with a jump instruction pointing to the virus code

Swiss Cheese Infection

- Viruses inject themselves into executable code
- Original code transferred and stored inside virus code
- Host code executes properly after the infection

Split Infection

- Virus splits into several parts
- Parts placed at random positions in host program
- Head of virus code starts at beginning of file
- Gives control to next piece of virus code

Malware that spread : Computer Virus

Types of Computer Virus

Program
- Infects executable files system

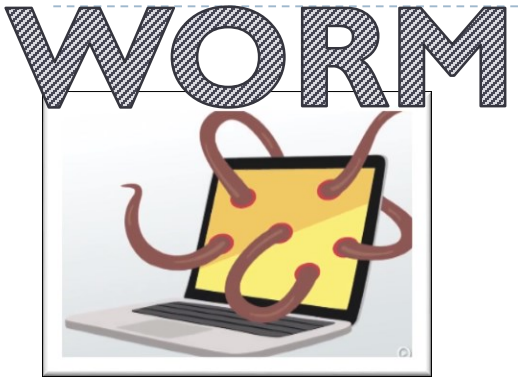
Macro
- Executes a script

Companion virus
- Adds malicious copycat program to operating system

Boot virus
- Infects the Master Boot Record

Resident
- Virus infects files opened by user or operating

Malware that spread : Worm



Computer worm very similar to the virus but worm are capable of moving from system to system without any human action

- Exploits application or operating system vulnerability
- Sends copies of itself to other network devices

Examples of worm actions

- Deleting computer files
- Allowing remote control of a computer by an attacker

Worms may:

- Consume resources or
- Leave behind a payload to harm infected systems

Malware that spread

Action	Virus	Worm
How does it spread to other computers?	Because viruses are attached to files, it is spread by a user transferring those files to other devices	Worms use a network to travel from one computer to another
How does it infect?	Viruses insert their code into a file	Worms exploit vulnerabilities in an application or operating system
Does there need to be user action?	Yes	No
Can it be remote controlled?	No	Yes

Difference between viruses and worms

Malware That Conceals: Trojan

- Type of malware that is often disguised as legitimate software.
- Trojans can be employed by cyber-thieves and hackers, trying to gain access to users' systems.
- Typically executable programs

- Contain hidden code that launches an attack

- Sometimes made to appear as data file
- Example
  - User downloads "free calendar program"
  - Program scans system for credit card numbers and passwords
  - Transmits information to attacker through network

Malware That Conceals: Rootkits

- Rootkits can be detected using programs that compare file contents with original files
- Rootkits that operate at operating system's lower levels:
  - May be difficult to detect
- Removal of a rootkit can be difficult
  - Rootkit must be erased
  - Original operating system files must be restored
  - Reformat hard drive and reinstall operating system

Malware That Conceals: Logic bomb / Backdoor

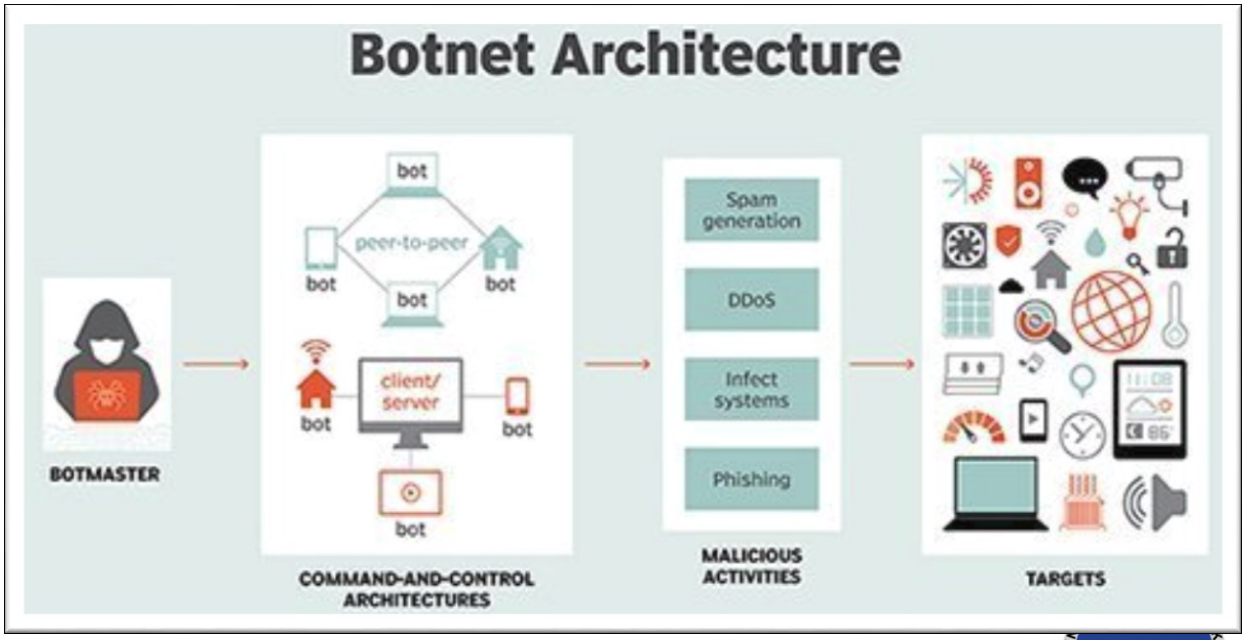
- One of the oldest types of malicious software
- Code embedded in legitimate program
- Activated when specified condition met
  - Eg: presence / absence of some file
  - Particular date/time
  - Particular user
- When triggered typically damage system
  - modify/delete files/disks, halt machine, etc.

- A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data. It denies normal authentication procedures to access a system.
- The backdoor access method is sometimes written by the programmer who develops a program.

Malware That Profits: Botnets

- The word Botnet is formed from the words 'robot' and 'network'
- A **botnet** is a group of computers connected in a coordinated fashion for malicious purposes.
- Each computer in a **botnet** is called a bot. **These** bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks

- Botnets' advantages for attackers
  - Operate in the background (Often with no visible evidence of existence)
  - Provide means for concealing actions of attacker
  - Can remain active for years



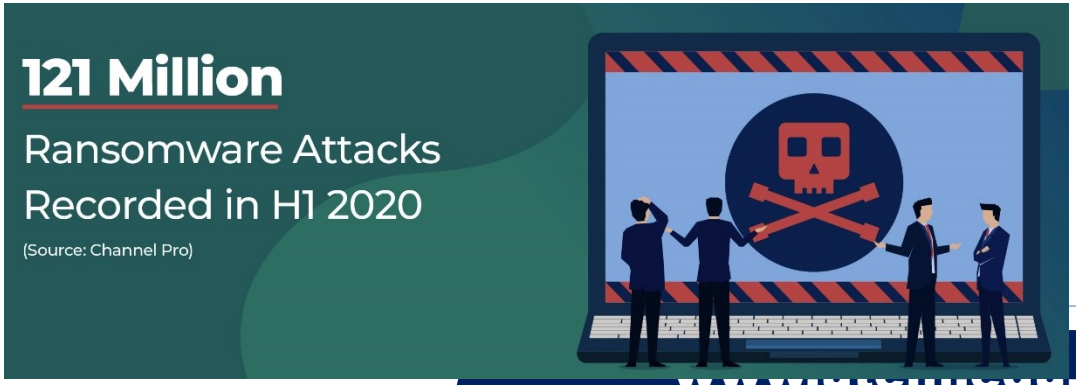
Malware That Profits: Botnets

Type of attack	Description
Spamming	A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam; some botnets can also harvest e-mail addresses
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets; zombies have the ability to download and execute a file sent by the attacker
Attacking IRC networks	Botnets are often used for attacks against IRC network; the bot herder orders each botnet to connect a large number of zombies to the IRC network, which is flooded by service requests and then cannot function
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person; online games can be manipulated in a similar way
Denying services	Botnets can flood a Web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests

Uses of botnets

Malware That Making Profits: Ransomware

- **Ransomware** is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.
- It infecting and taking control of the victim's machine, files or documents stored on it.
- Typically, the ransomware will either 'lock' the computer to prevent normal usage or encrypt the documents and files to prevent access to the saved data.
- Ransomware is usually installed when you open
  - A malicious email attachment
  - Click a malicious link in
    - An email message
    - An instant message
    - On social networking sites



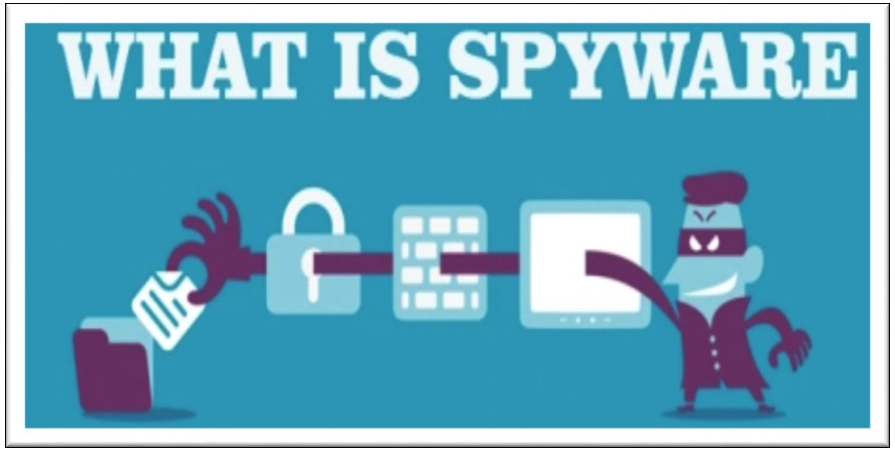
Malware That Profits: Spyware

- **Spyware** is software that is downloaded onto your computer to track your activities without your knowledge.
- Most of the time **spyware** is used to monitor your internet surfing habits, and this information is used in conjunction with adware to target specific advertisements to your tastes.
- Usually used for:

- Advertising - Collecting personal information - Changing computer configurations

- Spyware's negative effects

- Slows computer performance
- Causes system instability
- May install new browser menus or toolbars
- May place new shortcuts
- May hijack home page
- Causes increased pop-ups



Malware That Profits: Spyware

Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as Web sites a user has visited
System-modifying software	Modifies or changes user configurations, such as the Web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Technologies used by spyware

Malware That Profits: Adware

- The term **adware** is frequently used to describe a form of malware which presents unwanted advertisements to the user of a computer. The advertisements produced by **adware** are sometimes in the form of a pop-up or sometimes in an "unclosable window"
- Downsides of adware for users

- May display objectionable content
- Frequent pop-up ads cause lost productivity
- Pop-up ads slow computer or cause crashes
- Unwanted ads can be a annoyance

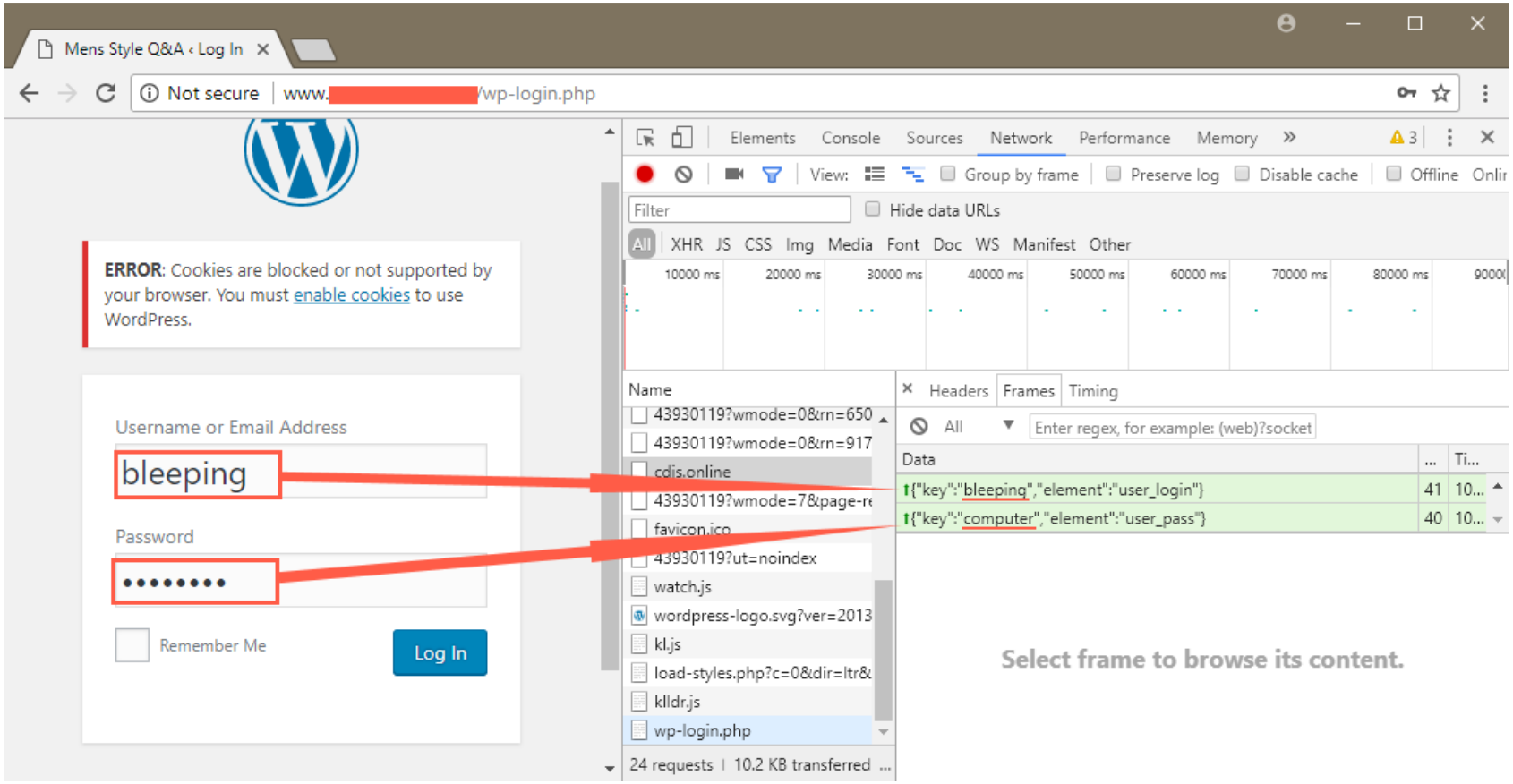
Malware That Profits: Keyloggers

Keyloggers
–Program that captures user's keystrokes
–Information later retrieved by attacker
–Attacker searches for useful information
•Passwords
•Credit card numbers
•Personal information

Hardware keylogger

Can be a small hardware device
•Inserted between computer keyboard and connector
•Unlikely to be detected
•Attacker physically removes device to collect information

Malware That Profits: Keyloggers

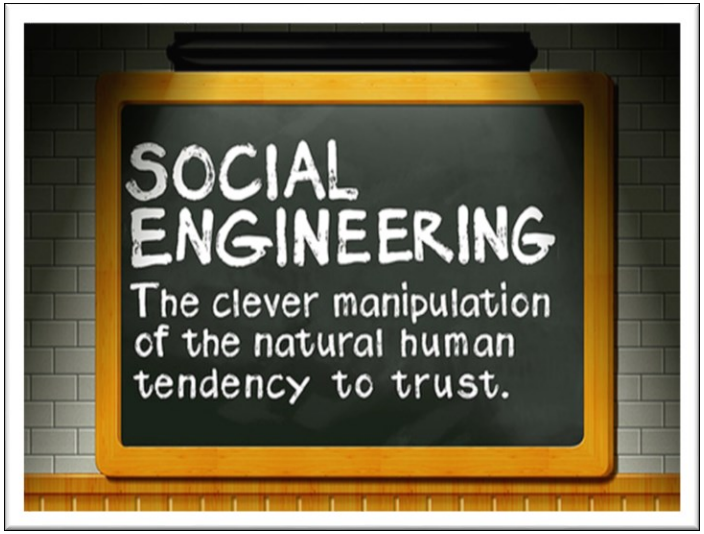


Information captured by a software keylogger

Social Engineering Attacks

- Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain

- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.



- Goal: persuade the victim to provide information or take action
  - Flattery or flirtation
  - Conformity
  - Friendliness

Social Engineering Attacks

- Types of Social Engineering attacks :

1. Phishing
2. Spam
3. Dumpster diving
4. Tailgating

Social Engineering Attacks : Phishing

- Sending an email claiming to be from legitimate source
  - May contain legitimate logos and wording
- Tries to trick user into giving private information

- Variations of phishing

1. **Pharming**
   - Automatically redirects user to fraudulent Web site
2. **Spear phishing**
   - Email messages target specific users
3. **Whaling**
   - Going after the "big fish"
   - Targeting wealthy individuals
4. **Vishing (voice phishing)**
   - Phone's version of email phishing and uses automated voice messages to steal confidential information.

   - Vishing video

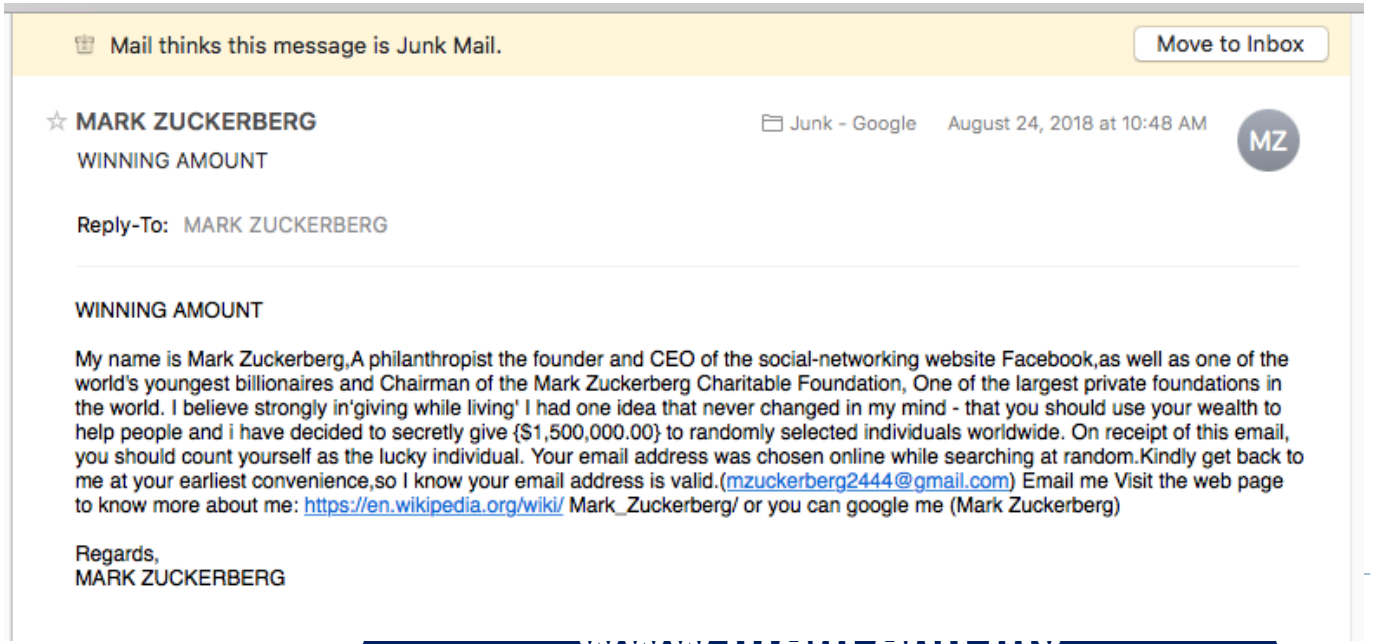
Social Engineering Attacks : Phishing

- Ways to recognize phishing messages
  - –Deceptive Web links
    - •@ sign in middle of address
  - –Variations of legitimate addresses
  - –Presence of vendor logos that look legitimate
  - –Fake sender's address
  - –Urgent request

Social Engineering Attacks : Spam

- Unwanted or unsolicited bulk e-mail
- Primary vehicles for distribution of malware

•Spim: targets instant messaging users
•Image spam
–Uses graphical images of text
–Circumvents text-based filters
–Often contains nonsense text



Social Engineering Attacks

- **Hoaxes**
  - –False warning or claim
  - –May be first step in an attack
- **Physical procedures**
  - –Dumpster diving
    - •Digging through trash to find useful information
  - –Tailgating
    - •Following behind an authorized individual through an access door

Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and may contain valuable information
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation
Organizational charts	These identify individuals within the organization who are in positions of authority
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate
Policy manuals	These may reveal the true level of security within the organization
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities

Dumpster diving items and their usefulness

Summary

- Malware is software that enters a computer system without the owner's knowledge or consent
- Malware that spreads include computer viruses and worms
- Malware that conceals include Trojans, rootkits, logic bombs, and backdoors
- Malware with a profit motive includes botnets, spyware, adware, and keyloggers
- Social engineering is a means of gathering information for an attack from individuals
- Types of social engineering approaches include phishing, impersonation, dumpster diving, and tailgating