

Lesson 27

Communications and Collaboration

**Computer Literacy
BASICS: A
Comprehensive Guide
to IC³, 4th Edition**

Objectives

- Explore communication methods.
- Identify the advantages of electronic communication.
- Solve electronic communication problems.
- Protect against viruses and other security risks.
- Engage in professional and effective communications.
- Use other e-mail options.
- Follow guidelines for electronic communication.

Vocabulary

- filtering
- fraud
- hoax
- logic bomb
- netiquette
- phishing
- pyramid scheme
- RDF Summary
- spam
- tagging
- teleconferencing
- time bomb
- Trojan horse
- urban legend
- virus
- worm

Exploring Communication Methods

- When you work with computers to communicate, you can use a variety of electronic communication methods, including e-mail and texting.



Exploring Communication Methods (continued)

- Teleconferencing uses a telecommunications system to serve groups, permitting the live exchange and sharing of information between two or more people.
- Syndication (Really Simple Syndication, or RSS), also known as Rich Site Summary and RDF Summary, are formats widely used to share the contents of blogs.

Identifying the Advantages of Electronic Communication

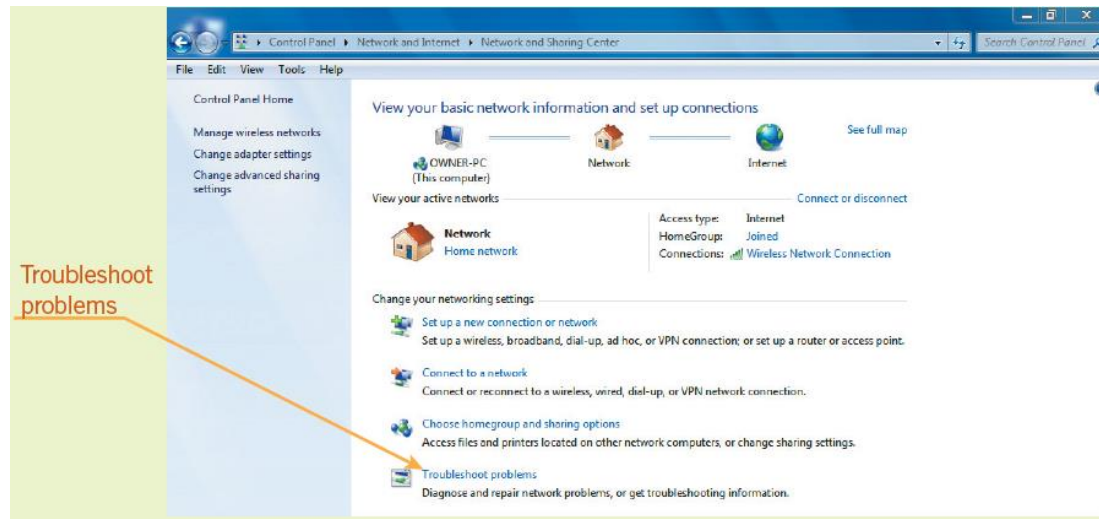
- Electronic communication offers many advantages over other types of communication:
 - Not restricted to a specific place and time
 - You can use text and graphics
 - You can use more than one type of correspondence
 - Fosters community building
 - Online document sharing

Identifying the Advantages of Electronic Communication (continued)

- Other advantages include:
 - Speed is almost instantaneous
 - Cost is minimal or even free
 - Access is available from various devices
 - Forwarding and routing of messages can be accomplished in an instant

Solving Electronic Communication Problems

- **Lost Internet Connection:**
- You may be able to repair the problem with the Internet Connections troubleshooter.



Solving Electronic Communication Problems (continued)

- **E-Mail Software Problems:**
- Your service provider's connection could be down.
- Often, waiting a few minutes and then trying to send or receive messages results in success.
- **Problems with Downloading and Viewing E-Mail Attachments:**
 - Attachment is too big or too many attachments
 - Antivirus software or e-mail program is blocking
 - Sender or type of e-mail is being blocked

Solving Electronic Communication Problems (continued)

- **Delivery Failure:**
- E-mail delivery failure refers to a returned or “bounced” e-mail.
- **Garbled Messages/No Guaranteed Delivery:**
- Occasionally, e-mail and other transmissions over the Internet are lost or spliced together.

Solving Electronic Communication Problems (continued)

- **Lost Formatting:**
- Not all e-mail programs support HTML-formatted messages, so formatting is lost.
- **Lack of a Paper Trail:**
- A paper trail is a written record, history, or collection of evidence created by a person or organization in the course of activities. Not all types provide this.
- **Hasty Responses:**
- Don't send quick replies that you might later regret.

Solving Electronic Communication Problems (continued)

Lesson 27

- **Professional and Informal Communication:**
- When writing professional communications, take time to be more formal.
- **Volume of E-Mail Replies:**
- Netiquette refers to good manners when communicating through electronic media.
- **Junk Mail (Spam):**
- Just as with regular mail, you might receive unsolicited messages in your inbox.

Solving Electronic Communication Problems (continued)

- **Frauds, Hoaxes, and Other False Information:**
- Electronic fraud is a computer crime that involves the manipulation of a computer or computer data to dishonestly obtain money, property, information, or other things of value, or to cause loss.
- Phishing messages are personal information scams.
- Pyramid schemes are an illicit business model where profits are based on the investor's ability to recruit other people who are enrolled to make payments to their recruiters.

Solving Electronic Communication Problems (continued)

- **Frauds, Hoaxes, and Other False Information (continued):**
- A hoax is an attempt to deceive an audience into believing that something false is real.
- Urban legends are stories that at one time could have been partially true but have grown from constant retelling into a mythical yarn.

Protecting Against Viruses and Other Security Risks

- **Viruses:**
- A program written to corrupt data on a computer.
 - A worm makes many copies of itself, consuming system resources so that the computer slows down or actually halts tasks.
 - A time bomb does not cause its damage until a certain date or until the system has been launched a certain number of times.

Protecting Against Viruses and Other Security Risks (continued)

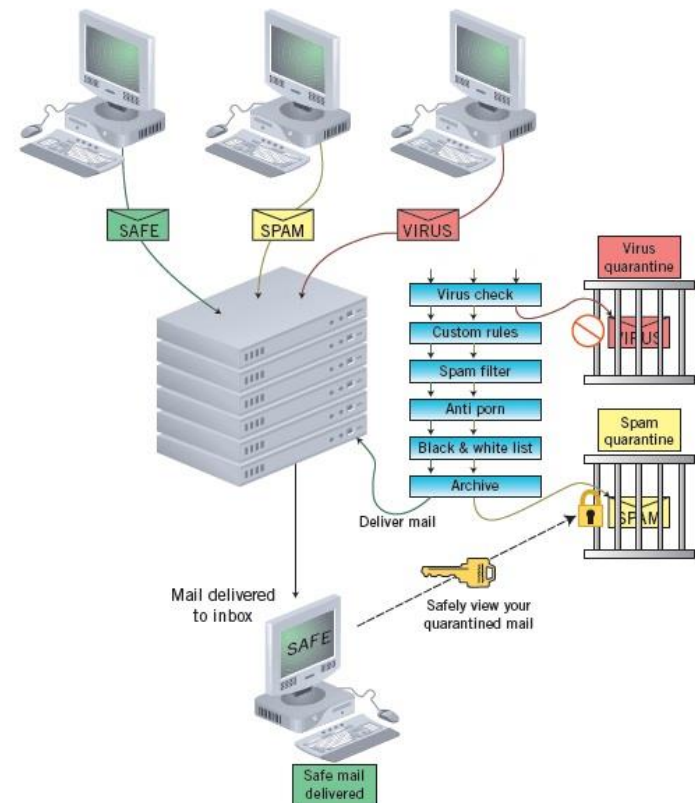
- **Viruses (continued):**
 - A logic bomb is triggered by the appearance or disappearance of specified data.
 - A Trojan horse is a virus that does something different from what it is expected to do.
- **General Security Risks:**
- The best way to protect data is to effectively control access to it using passwords, firewalls, or other methods.

Engaging in Professional and Effective Communications

- Content, tone, and format should be appropriate
- Personal and social messages can be less formal
- Select a method that suits the purpose
- Respond quickly
- Messages should be concise and to the point
- Include one subject per e-mail
- The purpose and recipients should determine the level of formality
- Don't duplicate or repeat information

Using Other E-Mail Options

- Control for viruses and spam.
- Protective tools and procedures include firewalls, encryption, antivirus tools, spam filters, and user education.



Using Other E-Mail Options

- **Controlling Unsolicited E-Mail:**
- You can filter your incoming e-mail messages to do the following:
 - Sort incoming messages into folders
 - Automatically tag messages
 - Forward messages
 - Discard messages

Using Other E-Mail Options (continued)

- **Filtering Mail by Mail Servers:**
- E-mail servers are usually set up to catch obvious spam and remove it before it is transferred to users.



Following Guidelines for Electronic Communication

- Check all messages for viruses
- Verify communication is appropriate before sending
- Apply rules of netiquette and other policies
- Encrypt e-mail messages
- Back up and archive correspondence
- Understand the sensitive nature of data sent online
- Be aware communication can leave an “electronic trail”
- Follow school and organization guidelines

Summary

In this lesson, you learned:

- Teleconferencing uses a telecommunications system to serve groups, permitting the live exchange and sharing of information between two or more people.
- Syndication (Really Simple Syndication or RSS), also known as Rich Site Summary and RDF Summary, are formats originally developed to facilitate the syndication of news articles.

Summary (continued)

- Electronic communication offers many advantages over other types of communication. For example, the communication is not restricted to a specific place and time. Secondly, in most instances, it uses text and graphics rather than voice. These tools also provide for different types of correspondence such as one to one, one to many, or many to many.

Summary (continued)

- Typical communication problems include failing to connect to the Internet or to your e-mail server. Being unable to download or view an e-mail attachment could be due to the size of the attachment, a virus in the message, the sender, or the type of e-mail.
- Communications netiquette, a combination of the words net and etiquette, refers to good manners and proper behaviors when communicating through electronic media.

Summary (continued)

- Fraud is a computer crime that involves manipulating a computer or computer data to dishonestly obtain money, property, or other things of value or to cause loss.
- A virus is a program that has been written, usually by a hacker, to corrupt data on a computer. The virus is attached to a file and then spreads from one file to another once the program is started.
- Computer security can keep hardware, software, and data safe from harm or destruction. The best way to protect data is to effectively control access to it.