Chapter 1 Notes: Getting Started With Digital Media

Nathan Warner

Jan 27, 2023

Learning Outcomes:

1. List the characteristics needed to become a skilled digital master.
2. Identify how to name and save a file.
3. Explain how to ensure digital security.
4. Practice the techniques for good keyboarding.

Key Terms:

- **Adware:** Software that displays unwanted advertisements
- **Cyber Predator:** A person who uses the Internet to make contact with others (usually with children and teens) in order to harm them
- **Digital Media:** any com-bination of audio, video, images, and text used to convey a message through technology
- **Encryption:** Converting text into an unreadable series of numbers and let-ters to protect information. Digital encryption uses soft-ware that can scramble and unscramble the data
- **Ergonomics:** A science that studies the best way to design a workplace for maximum safety and productivity
- **Hacker:** A person who finds an electronic means of gain-ing unauthorized access to a computer.
- **Keylogger:** Software that tracks keyboard use and transmits it to be used for illegal purposes
- **Malware:** The abbrevia-tion for malicious software, designed to damage a com-puter or steal information.
- **Naming Convention:** A set of rules used in the naming of files and folders
- **Online Backup:** A means of backing up or storing data using the Internet.
- **Phising:** A social engi-neering activity where the perpetrator uses fake websites or emails to trick a user into providing personal information or passwords
- **Repetitive Stress Injury:** Muscle or joint injury that results from performing actions repeatedly.
- **Rootkit:** Type of malware that hides its presence on a computer
- **Server:** A computer designed to store files from multiple computers
- **Social Engineering:** Tricking users into providing information in the belief that a request is legitimate.
- **Spyware:** Software that gathers information about a user without their knowledge
- **Trojan:** Type of malware that disguises itself as legitimate software
- **Virus:** Type of malware that replicates itself and spreads to other computers
- **Worm:** Type of malware that also replicates itself but primarily spreads through networks

Key Concepts:

- The five commitments to learning include: be flexible, keep an open mind, use initiative, listen and read attentively, and seek to acquire new knowledge and skills.
- The six behaviors that contribute to your ability to acquire a job and grow in the field of your choice include good attendance, promptness, proper attire, a clean and safe work environment, appropriate voice, and pride.
- You can demonstrate your digital media skills by seeking certification from a secondary and/or post-secondary school or through a provider such as Adobe or Microsoft.
- Managing digital files is an essential part of creating a good work environment.
- Strong passwords are those that meet a set of rules designed to make it difficult for others to figure out the word.
- Repetitive stress injury (RSI) (including carpal tunnel syndrome) results from repeated movement of a particular part of the body.

Commitment:

In order to learn new software and computer skills, you must:

- Be flexible
- Keep an open mind
- Use initiative
- Listen and read attentively
- Seek to acquire new knowledge and skills

Work Skills For Multimedia Careers:

- Good attendance
- Promptness
- Proper attire
- Clean and safe work environment
- Appropriate voice
- Pride

Managing Files:

Digital media projects often include multiple components as part of the final product. These may include image, text, audio, and video files. All must be saved in such a way and in such a place that anyone involved in the project can find the most current versions.

Naming Files:

The first step in managing files is deciding on a naming practice, or ***naming convention***. Choose a name that clearly identifies the contents of the file. If files are to be shared, the author's name or initials and some numbering method should be used to make sure the correct versions are apparent.

If a filename includes multiple words, one of two formats should be used.

- Link words with an underscore
- Link words with upper and lower case

Whitespace inbetween words should not be used because they can lead to problems down the road. They should especially be avoided in files that used in a web page because the linking process replaces empty spaces with %20, making the url address appear confusing when it is sited or referenced.

Note:-

Special symbols should also be avoided when naming files.

Saving Files:

You should also make sure save your files to the correct location. There should be a designated place to save project files, and everyone on a project team must know where that is.

Network locations or shared internet locations are often used to allow everyone access to the same material. Make sure you know where the shared folder is located. Make sure you know what file type is adequate for the file you are working on. This is especially important for image files.

Note:-

Make sure folder/file names are clearly identifiable.

Choosing Storage:

Video and image files can often be very large, it is important to know what demands these files are making on your system.

Organizations often store files on dedicated serves. **Dedicated servers** are one or more hard drives stored in a location seperate from the desktop computers used by employees. While servers storage limits are usually much higher than standard desktops, it is still important to take into consideration the size of the file that you are saving to the server.

Note:-

Another means of storage can be a writeable CD or DVD.

Flash drives are a means of storage that uses a circut board, unlike a hard drive which uses a spinning plater. Because flash drives use a circut board, this means that there are no moving parts to break. Flash drives are attached to a computer through the usb port. This makes it easy to transfer data from one machine to another.

Making Backups:

There are 3 main ways of creating backups:

- Backing up to a flash drive or another hard drive/external drive.
- **Online backup:** Files are transfered over the internet to a computer in a distant location.
- **Backup through the network:** Information is stored on another computer within the network.

Short term, more frequent backups can be made to removable media such as flash drives. Long term backups may be sent to an online server.

Personal Security:

It is important to protect yourself online. This means not revealing any personal information or providing information to sites that you do not trust. Online ***cyber predators*** who hunt for victims are dangerous to everyone. Not everyone is as they appear online. Even the most seemingly harmless exchange could lead to a dangerous situation.

Another danger is ***Identity Theft***. This is an issue for everyone who registers at websites, purchases items on the web, or uses social network sites. It is important to be aware of the more recent internet security issues. This includes the latest ***Social Engineering*** scams or keylogging tricks.

Computer Security:

Keeping your computer and network secure requires you to keep from dangers such as ***Maleware***. This is software that is downloaded on the victims computer without their knowledge, and with malicious intent.

Note:-

It is important to understand the distinctions between each of the hazards.

virus	A program that infects a computer without the permission or knowledge of the owner. A virus usually attaches itself to executable programs, allowing it to travel to other computers. Viruses require action by the computer user in order to activate them.
worm	A form of a virus that does not require any action by the computer user. It spreads by using the email functions of the computer. A worm's action overwhelms Web servers, often shutting them down.
spyware	Malware that captures information from a computer without the user's knowledge or consent.
Trojan horse (also called Trojan)	Software that appears to be useful but instead allows access to a computer without the user's knowledge or consent.
adware	Software that delivers advertising without the user's knowledge or consent.
rootkit	Software designed to keep a computer user from knowing the computer system has been infected by malware.

If you download software from the internet, make sure its from a secure site. You should also never open suspicious emails or unexpected attachments.

If you log into a public network, there is a potential risk to your computer. Some networks are more secure than others, meaning they have passwords and ***encryption***. Be careful what information you share over a network.

Note:-

Remember that no software protection can prevent a network hacker from stealing information shared over an open network.

Password Security:

One of the most effective ways to keep your computer safe is through wise passwords. If your password is easy to figure out, code hackers can easily gain access to your computer and its files.

It is important for you password to have each of the following:

- Have a minimum of eight characters
- Use both upper and lower case letters
- Use at least one number
- Use at least one special character

Note:-

Phising is when hackers send out realistic emails asking for information

Hardware Security:

Because of the nature of portable laptops, they can be easily stolen. Loss of the hardware is an obvious problem, but you also loose the information that was stored on the machine. This is why it is important to make frequent backups of your important data.

Note:-

It is important that you pay attention to a situation that might compromise your machine.

Acceptable use Policy (AUP)

Organizations often use AUP's to encourage digital safety and appropriate use of hardware and software. These written agreements must be signed to ensure safety for everyone that is using the network.

These agreements may include the following:

- Password selection requirements, including frequency of change.
- Software usage restriction.
- Netiquette rules, including prohibiton of inappropriate emailing or texting subjects.
- Limits on the use of systems or items that overtax the network.