

Being Safe, Secure and Productive With Computers

Instructor: Lamont Saunders

"Floppy disks are one of the easiest ways to transfer data from one location to another; however they are also the most unreliable."



The uses of floppy disks including zip disks are fast becoming outdated. Too many people trust this data storage medium to be stable and secure. When a floppy failure occurs, users often ask "how did this happen?"



The two most common reasons are:



1. Using a floppy disk in more than one computer will increase the likelihood of disk failure. This is due to the differences in alignment from one floppy drive to another and increased exposure to a dusty floppy drive.
2. Ejecting a disk that is still spinning will damage the disk; it does not matter if the floppy disk is reading or writing.

Here are some precautionary measures that can help prevent major data loss:

1. Keep the most current copy of all data on external media such as external hard drives, CDs or flash drives.
2. Do not expose media to extreme temperatures.
3. Never touch the surface of the actual disk; hold the disk by its external jacket.
4. Floppy disks should be kept dry. If a disk becomes wet, dry it off immediately. A wet disk can be useable again if left to dry completely.
5. Keep floppy disks away from anything magnetic.
6. Do not bend a floppy disk.



At present, stated **CD-R** and **DVD-R** lifetimes are only *estimates* based on accelerated aging tests as the technology has not been in existence long enough to verify the upper range. With proper care it is thought that CD-Rs should be readable one thousand times or more and have a shelf life of several hundred years. Unfortunately, *some common practices can reduce shelf life to only one or two years*. Therefore, it is important to handle and store CD-Rs properly if it is necessary to read them more than a year or so later.



Flash drives are nearly impervious to the scratches and dust that are problematic for compact discs and floppy disks, and their durable solid-state design means they often survive casual abuse. This makes them ideal for transporting personal data from one location to another or for carrying around personal data that the user typically wants to access in a variety of places. The universal use of USB on computers means that such a drive will work in most places.

Like all flash memory devices, flash drives can sustain only a limited number of write and erase cycles before failure. Mid-range flash drives under normal conditions will support several hundred thousand cycles, although write operations will gradually slow as the device ages.

Flash drives are more tolerant of abuse than mechanical drives, but can still be damaged or have data corrupted if an impact loosens circuit connections.

Being Safe, Secure and Productive With Computers

Instructor: Lamont Saunders

There are four main threats to online security.

- **Exploits that attack unpatched or old version programs.** A successful attack can give an intruder complete control of your computer and every bit of information on it.
- **Deceptive downloads.** Some of the nastiest bits of spyware and malware walk through the front door, disguised as or piggybacking along with benign or harmless-sounding programs.
- **Phishing attempts.** The most popular form of browser-based crime in 2007 is the phishing e-mail, which tries to sucker its victim into filling in valuable personal information – bank passwords, credit card details – in a phony web form.
- **Hostile add-ons.** A rogue program can be merely annoying – hijacking your home page and spewing unwanted pop-ups – or it can take the form of a Trojan horse or dialer that can drain its victim's bank account.



Anti virus programs:

AVG: <http://free.grisoft.com/>

Avast: www.avast.com

Symantec NAV: http://symantec.com/home_homeoffice/index.jsp

McAfee: <http://us.mcafee.com/>

Windows Live One Care: <http://www.windowsonecare.com/>

Anti Adware and Spyware software:

Adaware: www.lavasoftusa.com

Spybot Search and Destroy: www.safer-networking.org/en/download/index.html

ThreatFire: <http://www.threatfire.com/>

McAfee SiteAdvisor: <http://www.siteadvisor.com/>

SpywareBlaster: <http://www.javacoolsoftware.com/spywareblaster.html>

Windows Defender: <http://www.microsoft.com/athome/security/spyware/software/default.msp>

AVG anti-spyware Free: <http://free.grisoft.com/>



Being Safe, Secure and Productive With Computers

Instructor: Lamont Saunders

Content Filters:

Bsafe: www.bsafehome.com

Covenant Eyes: www.covenanteyes.com

CyberPatrol: <http://cyberpatrol.com/>

Cyber Sentinel: www.securitysoft.com

Cyber Sitter: www.solidoak.com

NetDog: www.netdogsoft.com

NetNanny: www.NetNanny.com

WiseChoice: www.wisechoice.net



Browsers:

Avant: <http://www.avantbrowser.com/>

Firefox: <http://www.mozilla.com/firefox/>
<http://www.mozilla.com/en-US/firefox/all-beta.html>

Opera: <http://www.opera.com/>

Internet Explorer 7: <http://www.microsoft.com/windows/ie/default.mspx>

Internet Explorer 6:

<http://www.microsoft.com/windows/ie/ie6/downloads/critical/ie6sp1/default.mspx>



In Summary:



1. Copy your data to more than one type of data storage media.
2. Keep all your copies up to date.
3. Be mindful of the environmental conditions of your stored media.

4. Don't expect your data to last more than 15 years in normal household conditions. No media lasts forever.
5. Integrate new forms of storage media as soon as feasibly possible.
6. No single program does everything.
7. Generally, stay away from "toolbars" as an add-on to a browser.



8. Update, Update, Update and don't forget to Update.
9. Get in the habit of turning your computer off at night.