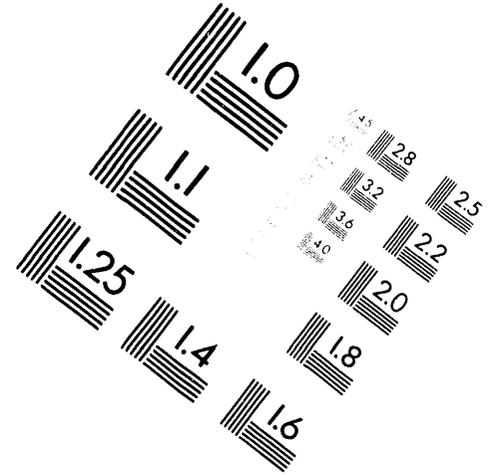
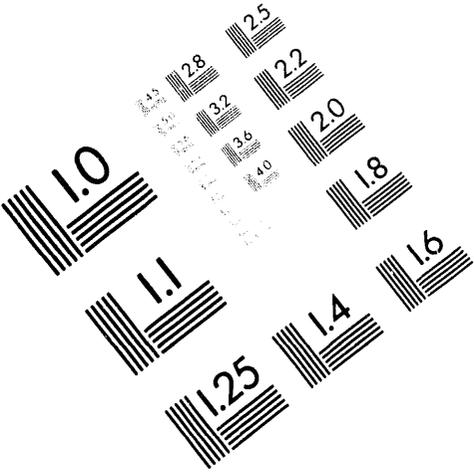




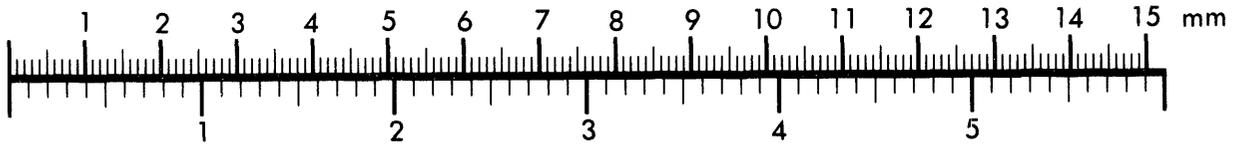
AIM

Association for Information and Image Management

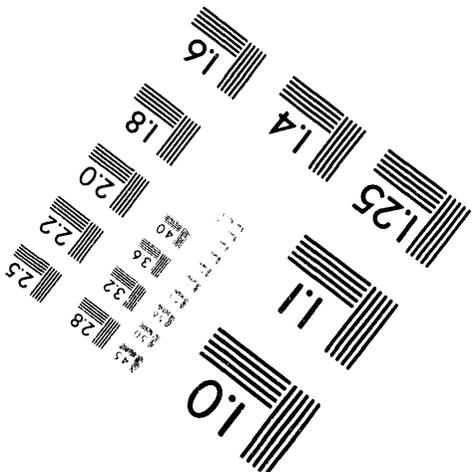
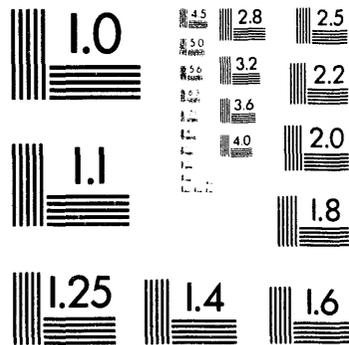
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202



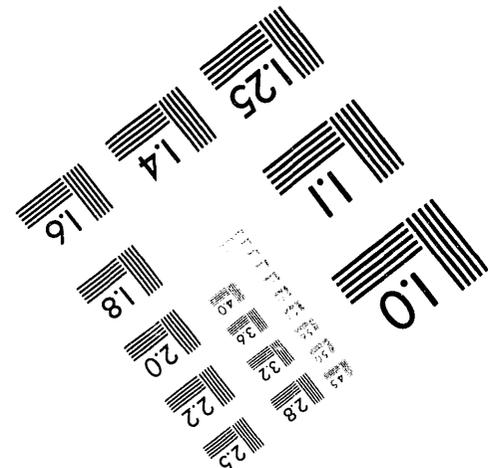
Centimeter

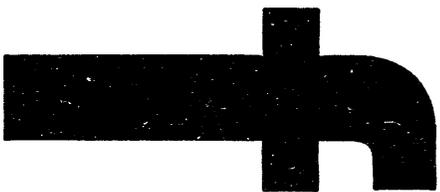
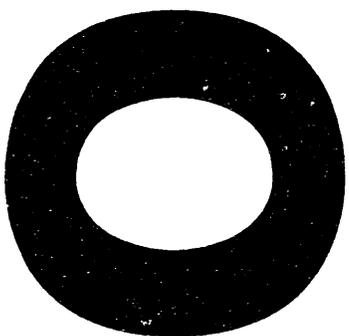


Inches



MANUFACTURED TO AIM STANDARDS
BY APPLIED IMAGE, INC.







Computer Security Awareness Guide

for

Department of Energy Laboratories,

Government Agencies, and others

for use with

Lawrence Livermore National Laboratory's (LLNL)

Computer Security Short Subjects Videos



MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

js

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

If any or all video segments are used in a video production or news broadcast, credit should be given to Lawrence Livermore National Laboratory.

Lawrence Livermore National Laboratory's Computer Security Short Subjects

Lonnie Moore, the Computer Security Manager, CSSM/CPM at Lawrence Livermore National Laboratory (LLNL) and Gale Warshawsky, the Coordinator for Computer Security Education & Awareness at LLNL, wanted to share topics such as computer ethics, software piracy, privacy issues, and protecting information in a format that would capture and hold an audience's attention. Four Computer Security Short Subject videos were produced which ranged from 1-3 minutes each. These videos are very effective education and awareness tools that can be used to generate discussions about computer security concerns and good computing practices.

Leaders may incorporate the Short Subjects into presentations. After talking about a subject area, one of the Short Subjects may be shown to highlight that subject matter. Another method for sharing them could be to show a Short Subject first and then lead a discussion about its topic.

The cast of characters and a bit of information about their personalities in the LLNL Computer Security Short Subjects follows.

Chip A computer who is a very likable fellow. Chip is the hero of the stories. Audiences identify with him and his frustrations in dealing with his users. This is a unique chance for you to get to experience the computer's point of view. Chip is fun loving, wise-cracking, sometimes mischievous, sometimes grouchy, very friendly, always hungry (for floppies), effervescent, bubbly, full of laughter and flirtatious (when infected with a virus). He likes to do lots of work, to be creative, to help users to compute safely and to be part of a team (computer-printer-network-human interface). He does not like goof offs, to be misused, to be ignored or messiness (he likes order).

Gooseberry A new computer user who wants to do what's right, but just can't get it. Gooseberry sees computers as "stupid machines." Gooseberry is giggly and goofy and makes many mistakes.

Dirty Dan A villain. He is an employee in any company, and may appear to be everyone's friend. However, he is truly up to no good. He is known to computer users as the "insider threat." He is dangerous and can cause much damage to your information. He is careless and messy.

A description of each of the Short Subject videos follows.

Hidden Password

Users must not leave their passwords lying about for others to discover. A password is like the key to your house. If the wrong person gets it, much damage could be caused. A thief could take many of the things you care about in your home. Information is very much like the items in your home. The information stored in our computers is very important and should be regarded as a valuable asset.

Gooseberry represents a new computer user. Poor Chip is at his wits' end as he observes Gooseberry making many bad decisions. The places Gooseberry thinks of hiding a password are the places that careless users actually do hide their passwords. Gooseberry never considers memorizing it.

Possible discussion topics:

Why would a computer user need to have a password?

(A password could be needed to access another computer where valuable data is stored. Protecting that information might require limited or controlled access to it).

Can you think of a good way to learn your password so you won't have to hide it?

(Brainstorm ideas with your users. The important thing to remember, is not to write down the password and hide it so someone else can use it.)

How can you make up a good password that nobody else could guess?

(Mix up alphabet letters and numbers so they make up a nonsense word or phrase that will be easy for you to remember, but hard for someone else to guess.)

The Incident

Dirty Dan represents the insider threat. Users who have sloppy computer security habits are among his targets. The unlocked door to your office is his invitation to come in and do his mischief. Are his deeds harmless, or can he cause you a great deal of trouble? Why should you log off when you are through using your computer, or before you leave your office?

Possible discussion topics:

Dirty Dan represents the insider threat. What kinds of damage might an insider do if he or she could get into your office?

(They could steal your ideas as well as your data. How often do many of us rough out ideas by writing them on a white board on the wall? The insider could also put a virus onto your personal computer.)

What can users do to protect their information from insider threats?

(Lock the door when leaving the office, logging off and not leaving terminals active, use software with password protection features, i.e., screen saver software.)

Dangerous Games

When a computer gets infected with a malicious program, such as a virus, the computer does not work as you expect it to. It may be impossible for you to use it until you get rid of the virus.

Possible discussion topics:

How do malicious software programs get onto floppy disks?

(Someone could write a malicious software program and put it onto a floppy disk. Someone could write a malicious software program and hide it inside another program. (This is called a Trojan horse). The Trojan horse could then be placed on a Bulletin Board System (BBS). A user can access a BBS and download the program they believe is meant to do word processing, spread sheet analysis, database management, graphics, or a game, etc. However, that program could contain the hidden virus (Trojan horse.) Typically a user would download that program to their computer's hard disk and make a copy of it on a floppy disk. When they go to use that program on their computer, their computer gets infected with the virus. If they put their floppy disk with the malicious program hidden on it into a friend's computer, and run the program, the friend's computer will also get infected with the virus.)

How easy is it for your computer to become infected?

(It is very easy to infect a computer. Sharing disks is not a good idea. If someone else's disk has a virus on it, and you use their disk in your computer, you would be putting the virus onto your computer.)

What can a user do to protect themselves and their computers against this threat?

(Use of virus protection/detection/eradication software programs, not sharing floppy disks, being careful when

accessing Bulletin Board Systems and not using illegal pirated software.)

The Mess

Poor Chip! Dirty Dan is at it again. He is so messy. Why can't he eat away from his computer? Why should Chip get full of his donut crumbs? Can food and drinks harm your computer?

Possible discussion topics:

Lead a discussion of the benefits of clean work areas. Why do you suppose food and drinks are not good for a computer? What kind of damage could happen if you spilled sofa or coffee on a computer or floppy disks?

(Food and drink can mess up the electronic parts in computers and floppy disks and then they won't work correctly. Soda spilled on a keyboard will make the keyboard sticky and the keys won't work properly. Other things, such as blocking the ventilation openings, cigarette smoke and cigarette ashes can also cause damage to a computer.)

A Note to Computer Security Education and Awareness Programs

This publication is part of the Lawrence Livermore National Laboratory (LLNL) Computer Security Education and Awareness Program. Computer Security at LLNL is part of the Computation Organization.

The Computer Security Short Subjects videos, featuring Chip, Gooseberry and Dirty Dan, were produced through the facilities of Images In Motion, Sonoma California. Images In Motion specializes in television-style creatures and animated objects and has major television and film credits.

BIOGRAPHIES

Lonnie R. Moore is the Computer Security Manager, CSSM/CPPM at Lawrence Livermore National Laboratory. He was awarded his BA in Political Science from California State University at Hayward in 1979, and he minored in Law. Mr. Moore has experience in all phases of computer and communications security, including management, planning, personnel, physical, communications, administration, incident investigations, and inspections. His career has also encompassed positions in all topics of Safeguards and Security including Protective Force Operations, Emergency Response Team Operations, Technical and Alarm Systems (design and operations), TSCM, Personnel, Security Awareness and Education, Information Security, Document Control, Test Site Security Operations, Investigations, Emergency Operations Management, Risk Analysis and Management. Mr. Moore served on government and contractor committees and working groups establishing policy and regulations for various Orders, guides, directives, manuals, standards and criteria. He is an avid public speaker, and participates regularly at seminars, conferences, and education courses as an individual speaker and panel participant. He was instrumental in designing and implementing the Computer Security Outreach Program for children in grades K-3.

Gale S. Warshawsky is the Coordinator for Computer Security Education and Awareness at Lawrence Livermore National Laboratory. She was awarded her MS in Information Systems from Golden Gate University 1991 and her BA in Theatre Arts Drama from San Jose State University 1979. Ms. Warshawsky is responsible for providing the Laboratory's personnel with education and awareness about computer security to meet the Department of Energy's requirements. She designs and gives presentations, writes a variety of awareness newsletters, announcements and bulletins, and organizes computer security training programs. Ms. Warshawsky is a frequent presenter at computer security and information science conferences. She also serves as a guest lecturer at Golden Gate University for a variety of graduate level courses in Information Systems and Telecommunications. She is a member of the Computer Security Institute (CSI), Information Systems Security Association (ISSA), Federal Information Systems Security Educator's Association (FISSEA), and the American Society for Information Science (ASIS). She was instrumental in designing and implementing the Computer Security Outreach Program for children in grades K-3. Ms. Warshawsky is also a member of Puppeteers of America and the San Francisco Bay Area Puppeteers Guild. She is the author of *Creative Puppetry for Jewish Kids* © 1985, Alternatives In Religious Education.



Leader's Guide
for Adult Computer Security Awareness Programs
for use with
The Computer Security Short Subject Videos

Lawrence Livermore National Laboratory's Computer Security Short Subject Videos

Lonnie Moore and Gale Warshawsky wanted to share topics such as computer ethics, software piracy, privacy issues, and protecting information in a format that would capture and hold an audience's attention. Four Computer Security Short Subject videos were produced which ranged from one to three minutes each. These videos are very effective education and awareness tools that can be used to generate discussions about computer security concerns and good computing practices.

Leaders may incorporate the Short Subjects into presentations. After talking about a subject area, one of the Short Subjects may be shown to highlight that subject matter. Another method for sharing them could be to show a Short Subject first and then lead a discussion about its topic.

The cast of characters and a bit of information about their personalities in The Computer Security Short Subjects follows.

Chip A computer who is a very likable fellow. Chip is the hero of the stories. Audiences identify with him and his frustrations in dealing with his users. This is a unique chance for you to get to experience the computer's point of view. Chip is fun loving, wise-cracking, sometimes mischievous, sometimes grouchy, very friendly, always hungry (for floppies), effervescent, bubbly, full of laughter and flirtatious (when infected with a virus). He likes to do lots of work, to be creative, to help users to compute safely and to be part of a team (computer-printer-network-human interface). He does not like goof offs, to be misused, to be ignored or messiness (he likes order).

Gooseberry A new computer user who wants to do what's right, but just can't get it. Gooseberry sees computers as "stupid machines." Gooseberry is giggly and goofy and makes many mistakes.

Dirty Dan A villain. He is an employee in any company, and may appear to be everyone's friend. However, he is truly up to no good. He is known to computer users as the "insider threat." He is dangerous and can cause much damage to your information. He is careless and messy.

The Short Subject videos were produced under the production facilities of Images In Motion.

A description of each of the Short Subject videos follows.

Hidden Password

Users must not leave their passwords lying about for others to discover. A password is like the key to your house. If the wrong person gets it, much damage could be caused. A thief could take many of the things you care about in your home. Information is very much like the items in your home. The information stored in our computers is very important and should be regarded as a valuable asset.

Gooseberry represents a new computer user. Poor Chip is at his wits' end as he observes Gooseberry making many bad decisions. The places Gooseberry thinks of hiding a password are the places that careless users actually do hide their passwords. Gooseberry never considers memorizing it.

Possible discussion topics:

Why would a computer user need to have a password?

(A password could be needed to access another computer where valuable data is stored. Protecting that information might require limited or controlled access to it).

Can you think of a good way to learn your password so you won't have to hide it?

(Brainstorm ideas with your users. The important thing to remember, is not to write down the password and hide it so someone else can use it.)

How can you make up a good password that nobody else could guess?

(Mix up alphabet letters and numbers so they make up a nonsense word or phrase that will be easy for you to remember, but hard for someone else to guess.)

The Incident

Dirty Dan represents the insider threat. Users who have sloppy computer security habits are among his targets. The unlocked door to your office is his invitation to come in and do his mischief. Are his deeds harmless, or can he cause you a great deal of trouble? Why should you log off when you are through using your computer, or before you leave your office?

Possible discussion topics:

Dirty Dan represents the insider threat. What kinds of damage might an insider do if he or she could get into your office?

(They could steal your ideas as well as your data. How often do many of us rough out ideas by writing them on a white board on the wall? The insider could also put a virus onto your personal computer.)

What can users do to protect their information from insider threats?

(Lock the door when leaving the office, logging off and not leaving terminals active, use software with password protection features, i.e., screen saver software.)

Dangerous Games

When a computer gets infected with a malicious program, such as a virus, the computer does not work as you expect it to. It may be impossible for you to use it until you get rid of the virus.

Possible discussion topics:

How do malicious software programs get onto floppy disks?

(Someone could write a malicious software program and put it onto a floppy disk. Someone could write a malicious software program and hide it inside another program. (This is called a Trojan horse). The Trojan horse could then be placed on a Bulletin Board System (BBS). A user can access a BBS and download the program they believe is meant to do word processing, spread sheet analysis, database management, graphics, or a game, etc. However, that program could contain the hidden virus (Trojan horse.) Typically a user would download that program to their computer's hard disk and make a copy of it on a floppy disk. When they go to use that program on their computer, their computer gets infected with the virus. If they put their floppy disk with the malicious program hidden on it into a friend's computer, and run the program, the friend's computer will also get infected with the virus.)

How easy is it for your computer to become infected?

(It is very easy to infect a computer. Sharing disks is not a good idea. If someone else's disk has a virus on it, and you use their disk in your computer, you would be putting the virus onto your computer.)

What can a user do to protect themselves and their computers against this threat?

(Use of virus protection/detection/eradication software programs, not sharing floppy disks, being careful when accessing Bulletin Board Systems and not using illegal pirated software.)

The Mess

Poor Chip! Dirty Dan is at it again. He is so messy. Why can't he eat away from his computer? Why should Chip get full of his donut crumbs? Can food and drinks harm your computer?

Possible discussion topics:

Lead a discussion of the benefits of clean work areas. Why do you suppose food and drinks are not good for a computer? What kind of damage could happen if you spilled soda or coffee on a computer or floppy disks?

(Food and drink can mess up the electronic parts in computers and floppy disks and then they won't work correctly. Soda spilled on a keyboard will make the keyboard sticky and the keys won't work properly. Other things, such as blocking the ventilation openings, cigarette smoke and cigarette ashes can also cause damage to a computer.)

A Note to Computer Security Education and Awareness Programs

The Computer Security Short Subject videos and this accompanying Leader's Guide, were written and produced for use in Computer Security Education and Awareness Programs.

The Computer Security Short Subject videos, featuring Chip, Gooseberry and Dirty Dan, were produced through the facilities of Images In Motion, Sonoma California. Images In Motion specializes in television-style creatures and animated objects and has major television and film credits.

BIOGRAPHIES

Lonnie R. Moore has many years experience as a computer security practitioner including managing the Lawrence Livermore National Laboratory's Computer Security organization. He was awarded his BA in Political Science from California State University at Hayward in 1979, and he minored in Law. Mr. Moore has experience in all phases of computer and communications security, including management, planning, personnel, physical, communications, administration, incident investigations, and inspections. His career has also encompassed positions in all topics of Safeguards and Security including Protective Force Operations, Emergency Response Team Operations, Technical and Alarm Systems (design and operations), TSCM, Personnel, Security Awareness and Education, Information Security, Document Control, Test Site Security Operations, Investigations, Emergency Operations Management, Risk Analysis and Management. Mr. Moore served on government and contractor committees and working groups establishing policy and regulations for various Orders, guides, directives, manuals, standards and criteria. He is an avid public speaker, and participates regularly at seminars, conferences, and education courses as an individual speaker and panel participant. He was instrumental in designing and implementing the Computer Security Outreach Kit for children in grades K-3.

Gale S. Warshawsky is the Coordinator for Computer Security Education and Awareness at Lawrence Livermore National Laboratory. She was awarded her MS in Information Systems from Golden Gate University 1991 and her BA in Theatre Arts Drama from San Jose State University 1979. Ms. Warshawsky is responsible for providing the Laboratory's personnel with education and awareness about computer security to meet the Department of Energy's requirements. She designs and gives presentations, writes a variety of awareness newsletters, announcements and bulletins, and organizes computer security training programs. Ms. Warshawsky is a frequent presenter at computer security and information science conferences. She also serves as a guest lecturer at Golden Gate University for a variety of graduate level courses in Information Systems and Telecommunications. She is a member of the American Society for Information Science (ASIS), Federal Information Systems Security Educator's Association (FISSEA), Computer Security Institute (CSI), and the Information Systems Security Association (ISSA). Gale Warshawsky was honored as ISSA's 1994 Security Practitioner of the Year. She was instrumental in designing and implementing the Computer Security Outreach Kit for children in grades K-3. Ms. Warshawsky is also a member of Puppeteers of America and the San Francisco Bay Area Puppeteers Guild. She is the author of *Creative Puppetry for Jewish Kids*, © 1985, Alternatives In Religious Education.

Acknowledgment of Government Sponsorship and License Rights

NOTICE: The Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, and perform publicly and display publicly. Beginning five (5) years after March 31, 1994, the Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this date to reproduce, prepare derivative works, distribute copies to the public, perform publicly and display publicly, and to permit others to do so.

NEITHER THE UNITED STATES NOR THE UNITED STATES DEPARTMENT OF ENERGY, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OF IMPLIED OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS.

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-ENG-48. UCRL-MI-113637

© 1993 The Regents of the University of California



Teacher's Guide for Elementary Schools
for use with
The Computer Security Short Subject Videos
by
Gale Warshawsky and Lonnie Moore

Lawrence Livermore National Laboratory's Computer Security Short Subject videos

Lonnie Moore and Gale Warshawsky wanted to share topics such as computer ethics, software piracy, privacy issues, and protection information in a format that would capture and hold an audience's attention. Four Computer Security Short Subject videos were produced which ranged from 1-3 minutes each. These videos are very effective education and awareness tools that can be used to generate discussions about computer security concerns and good computing practices.

Teachers may incorporate the Short Subject videos into presentations. After talking about a subject area, one of the Short Subjects may be shown to highlight that subject matter. Another method for sharing them could be to show a Short Subject first and then lead a discussion about its topic.

The cast of characters and a bit of information about their personalities in the LLNL Computer Security Short Subject videos follows:

Chip A computer who is a very likable fellow. Chip is the hero of the stories. Audiences identify with him and his frustrations in dealing with his users. This is a unique chance for you to get to experience the computer's point of view. Chip is fun loving, wise-cracking, sometimes mischievous, sometimes grouchy, very friendly, always hungry (for floppies), effervescent, bubbly, full of laughter and flirtatious (when infected with a virus). He likes to do much work, to be creative, to help users to compute safely and to be part of a team (computer-printer-network-human interface). He does not like goof offs, to be misused, to be ignored or messiness (he likes order).

Gooseberry A new computer user who is careless and makes many mistakes. Gooseberry sees computers as "stupid machines." Gooseberry's favorite food is pie. Gooseberry is fun loving and does not take life or anything else seriously.

Dirty Dan A real bad dude in the worst way. He is a real sleazy character and may appear to be everyone's friend. However, he is truly up to no good. He can cause much damage to your information. He is careless and messy.

The Short Subject videos were produced under the production facilities of Images In Motion.

A description of each Short Subject follows along with possible topics for discussion.

Hidden Password

Users must not leave their passwords lying about for others to discover. A password is like the key to your house. If the wrong person gets it, much damage could be caused. A thief could take many of the things you care about in your home. Information is very much like the items in your home. The information stored in our computers is very important and should be regarded as a valuable asset.

Gooseberry represents a new computer user. Poor Chip is at his wits' end as he observes Gooseberry being careless and making many bad decisions. The places Gooseberry thinks of hiding a password are the places that careless users actually do hide their passwords. Gooseberry never considers memorizing it.

Possible discussion topics:

Why would a computer user need to have a password?

(A password could be needed to access another computer. Many of your students may have heard of the Prodigy information service. Some of them may even be Prodigy users. To use Prodigy one needs a personal computer, communications software, a modem and the Prodigy software. It might be possible to arrange for a demonstration by Prodigy to show the children how connecting to an information service, such as Prodigy, requires a password).

Can you think of a good way to learn your password so you won't have to hide it?

(Brainstorm ideas with students. The important thing to remember, is not to be careless with your password. If students cannot memorize their password, is there an acceptable place for them to store it? Does the teacher have someplace that the passwords could be locked up?)

How can you make up a good password that nobody else could guess?

(Mix up alphabet letters and numbers so they make up a nonsense word or phrase that will be easy for you to remember, but hard for someone else to guess.)

The Incident

Dirty Dan represents the insider threat. Users who have sloppy computer security habits are among his targets. The unlocked door to your computer room at school is his invitation to come in and do his mischief. Are his deeds harmless, or can he cause a great deal of trouble? What's the big deal of leaving your computer room unsecured anyway?

Possible discussion topics:

What things did Dirty Dan do that were not very nice to Gooseberry's information on the computer?

(He looked at Gooseberry's school work, copied some of it and erased some of it.)

Is it okay for someone to take something that does not belong to them? How would you feel if someone took something that belonged to you?

(Lead a discussion about honesty and privacy. Compare taking data/information with taking something that belongs to the children. For example, how would they feel if someone took their bicycle? Would it matter if the thief took it forever or just for a short ride? How would the children react if someone took their diary, a painting they made for their parent, their homework, or letters they received from their friends? In each of these cases, the owner of the item, whether it be a bicycle, something the child drew or wrote, or a letter they received from a friend, gets deprived of the thing they own. This is the same loss a computer user might feel if a thief stole their information from their computer.)

How do you feel about what Dirty Dan did to Gooseberry's school work on the computer?

(Get the students to share their feelings on this. He not only made a copy of it for himself to show to his friends, but he also erased part of the information.)

What could Gooseberry have done to make sure the information on the computer could not have been messed up by someone else?

(Gooseberry could have saved and closed the file. Gooseberry could have used password protection software that would have not permitted someone not knowing Gooseberry's password to look at the information on the computer. Gooseberry could have locked the door to the computer room at school, when it was time to go eat lunch.)

Dangerous Games

What happens when a computer gets a virus? Will it behave normally? What effect can a malicious software program have on a computer user? How does Chip respond once he has been infected?

Possible discussion topics:

What is a computer virus?

(It is a malicious software program designed to make a computer not work properly. When children get sick with a virus they cough and sneeze. Sometimes they don't feel like playing. When a computer gets infected with a virus, it does not work well either. Once a computer gets infected with a virus it may be impossible to do anything on it! You would not be able to play games, print out your typing or pictures or even do your homework. The computer would stay infected until someone was able to remove the virus from it.)

How do malicious software programs get onto floppy disks?

(Someone could write a malicious software program and put it onto a floppy disk. Someone could write a malicious software program and hide it inside another program. (This is called a Trojan horse). The Trojan horse could then be placed on a Bulletin Board System (BBS). A user can access a BBS and download the program they believe is meant to do word processing, spread sheet analysis, database management, graphics, or a game, etc. However, that program could contain the hidden virus (Trojan horse). Typically a user would download that program to their computer's hard disk and make a copy of it on a floppy disk. When they go to use that program on their computer, their computer gets infected with the virus. If they put their floppy disk with the malicious program hidden on it into a friend's computer, and run the program, the friend's computer will also get infected with the virus).

How easy is it for your computer to become infected?

(It is very easy to infect a computer. Sharing disks is not a good idea. If someone else's disk has a virus on it, and you use their disk in your computer, you would be putting the virus onto your computer.)

What can a user do to protect themselves and their computers against this threat?

(Use of virus protection/detection/eradication software programs, not sharing floppy disks, being careful when accessing Bulletin Board Systems and not using illegal pirated software.)

The Mess

Poor Chip! Dirty Dan is at it again. He is so messy. Why can't he eat away from his computer? Why should Chip get full of his donut crumbs? Can food and drink harm your computer?

Possible discussion topics:

Why do you suppose food and drinks are not good for a computer? What kind of damage could happen if you spilled a drink on a computer or floppy disks?

(Food and drinks can mess up the electronic parts in computers and floppy disks and then they won't work correctly. Other things, such as blocking the ventilation openings, cigarette smoke and cigarette ashes can also cause damage to a computer.)

A Note to Teachers

These Short Subject videos are appropriate for viewing by children and adults. Some very interesting discussions could develop from viewing them. One of the concerns we have as computer security professionals, is that children are not being taught the ethics involved in using computers. Computer criminals try to break into computers at very young ages. By the time they are teenagers they become very good at breaking into computers and cause millions of dollars worth of damage. While we applaud educating children in the use of technology afforded us by living in the Information Age, we urge you to also address concerns such as respecting the property of others, even if that property is in electronic form. The ethics of using computers must become a part of the computer age. Perhaps if we educate our children early enough, we will have fewer instances of people breaking into computer systems later on.

The coloring book also features our hero Chip. It was designed for children in grades K-3. We made it very "child-friendly." Our aim with this coloring book was to provide very young children with a fun way to begin to learn about computers.

BIOGRAPHIES

Lonnie R. Moore has many years experience as a computer security practitioner including managing the Lawrence Livermore National Laboratory's Computer Security organization. He was awarded his BA in Political Science from California State University at Hayward in 1979, and he minored in Law. Mr. Moore has experience in all phases of computer and communications security, including management, planning, personnel, physical, communications, administration, incident investigations, and inspections. His career has also encompassed positions in all topics of Safeguards and Security including Protective Force Operations, Emergency Response Team Operations, Technical and Alarm Systems (design and operations), TSCM, Personnel, Security Awareness and Education, Information Security, Document Control, Test Site Security Operations, Investigations, Emergency Operations Management, Risk Analysis and Management. Mr. Moore served on government and contractor committees and working groups establishing policy and regulations for various Orders, guides, directives, manuals, standards and criteria. He is an avid public speaker, and participates regularly at seminars, conferences, and education courses as an individual speaker and panel participant.

Gale S. Warshawsky is the Coordinator for Computer Security Education and Awareness at Lawrence Livermore National Laboratory. She was awarded her MS in Information Systems from Golden Gate University 1991 and her BA in Theatre Arts Drama from San Jose State University 1979. Ms. Warshawsky is responsible for providing the Laboratory's personnel with education and awareness about computer security to meet the Department of Energy's requirements. She designs and gives presentations, writes a variety of awareness newsletters, announcements and bulletins, and organizes computer security training programs. Ms. Warshawsky is a frequent presenter at computer security and information science conferences. She also serves as a guest lecturer at Golden Gate University for a variety of graduate level courses in Information Systems and Telecommunications. She is a member of the American Society for Information Science (ASIS), Federal Information Systems Security Educator's Association (FISSEA), Computer Security Institute (CSI), and the Information Systems Security Association (ISSA). Gale Warshawsky was honored as ISSA's 1994 Security Practitioner of the Year. Ms. Warshawsky is also a member of Puppeteers of America and the San Francisco Bay Area Puppeteers Guild. She is the author of *Creative Puppetry for Jewish Kids*, ,, 1985, *Alternatives In Religious Education*.

Acknowledgment of Government Sponsorship and License Rights

NOTICE: The Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, and perform publicly and display publicly. Beginning five (5) years after March 31, 1994, the Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, distribute copies to the public, perform publicly and display publicly, and to permit others to do so.

NEITHER THE UNITED STATES NOR THE UNITED STATES DEPARTMENT OF ENERGY, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS.

Disclaimer

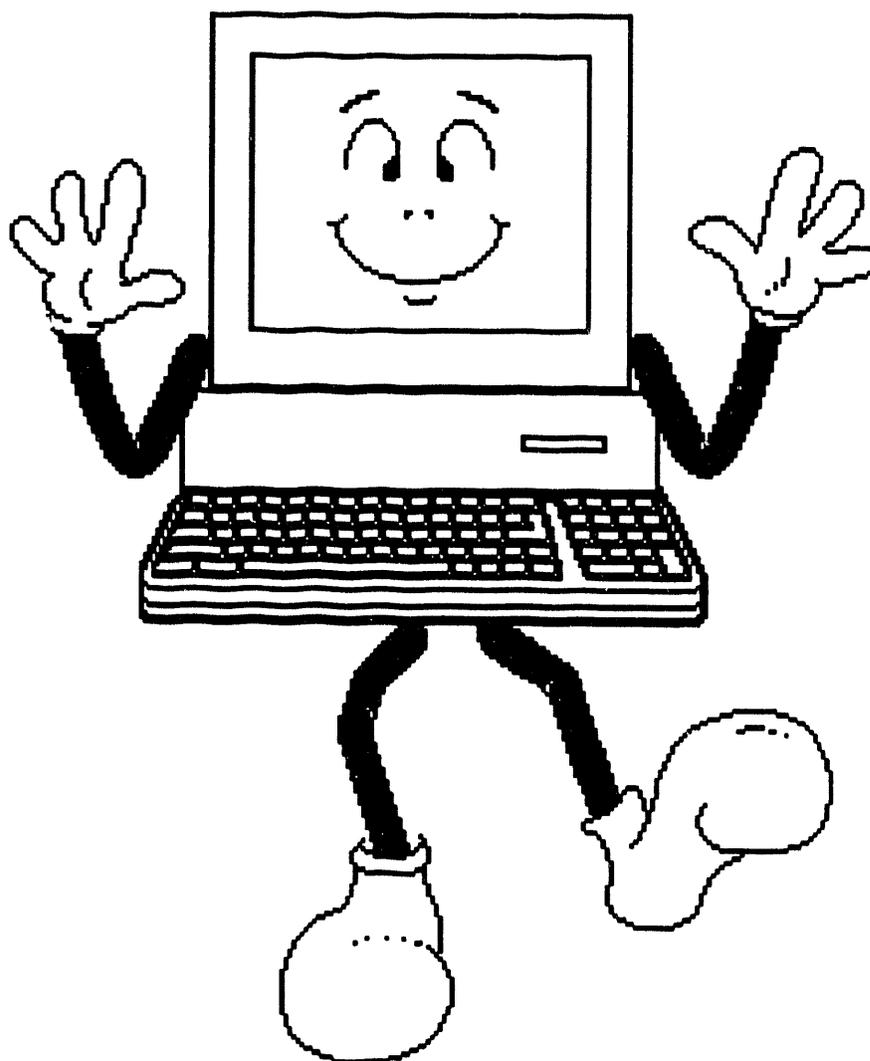
This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-ENG-48. UCRL-MI-113637

© 1993 The Regents of the University of California

Chip's Coloring Book

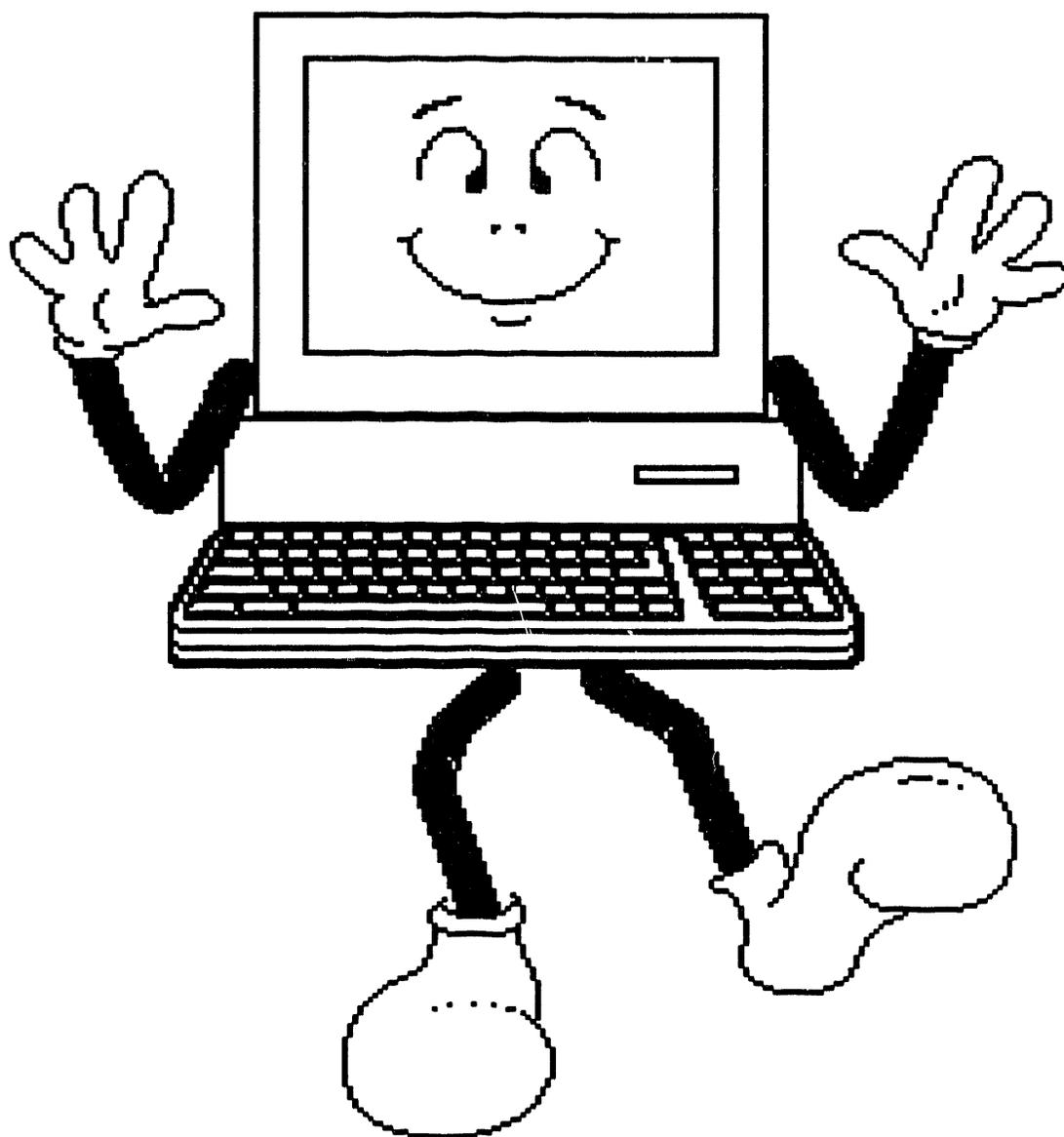
Hi. I'm Chip.
Let's color.

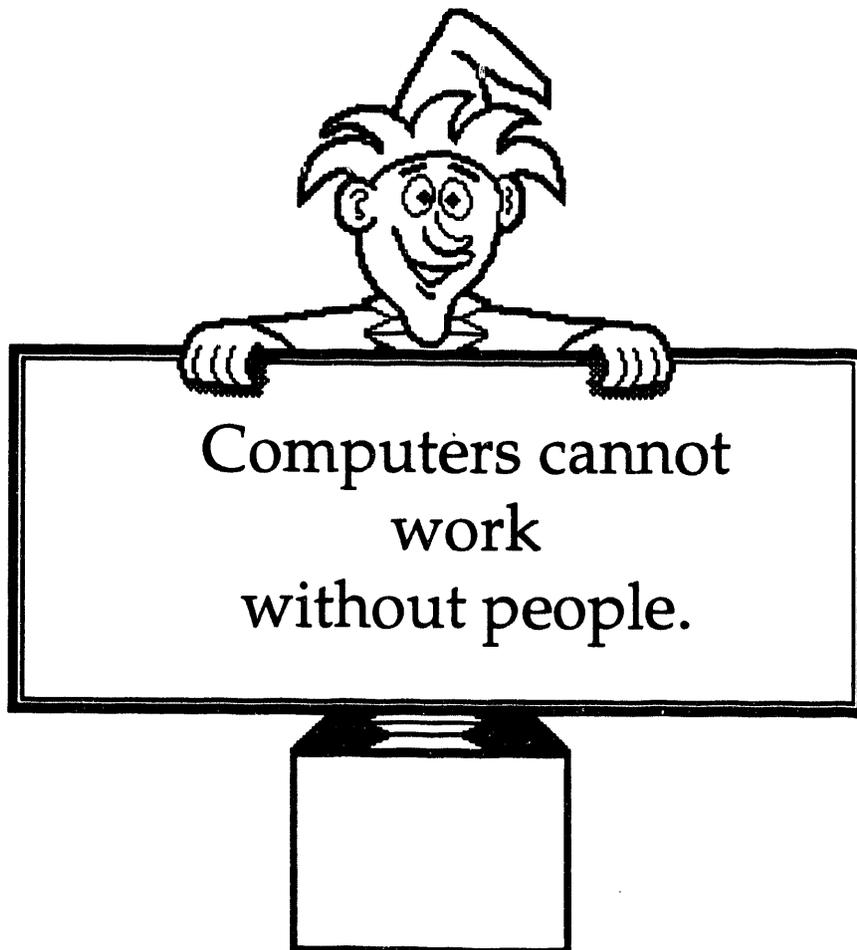
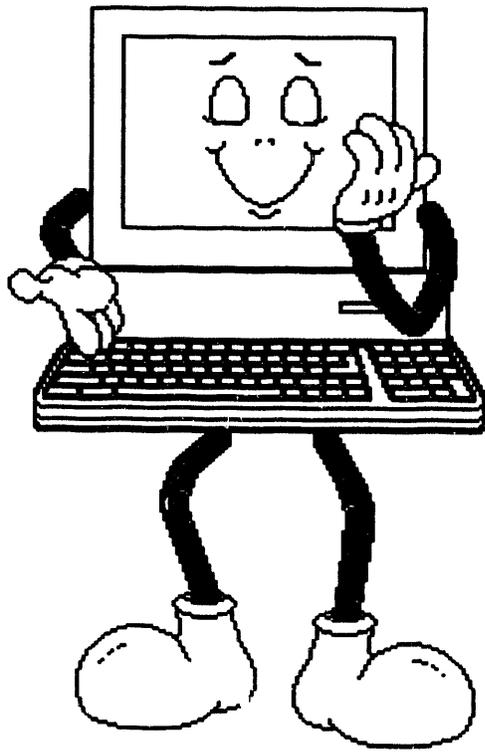


Lawrence Livermore National Laboratory

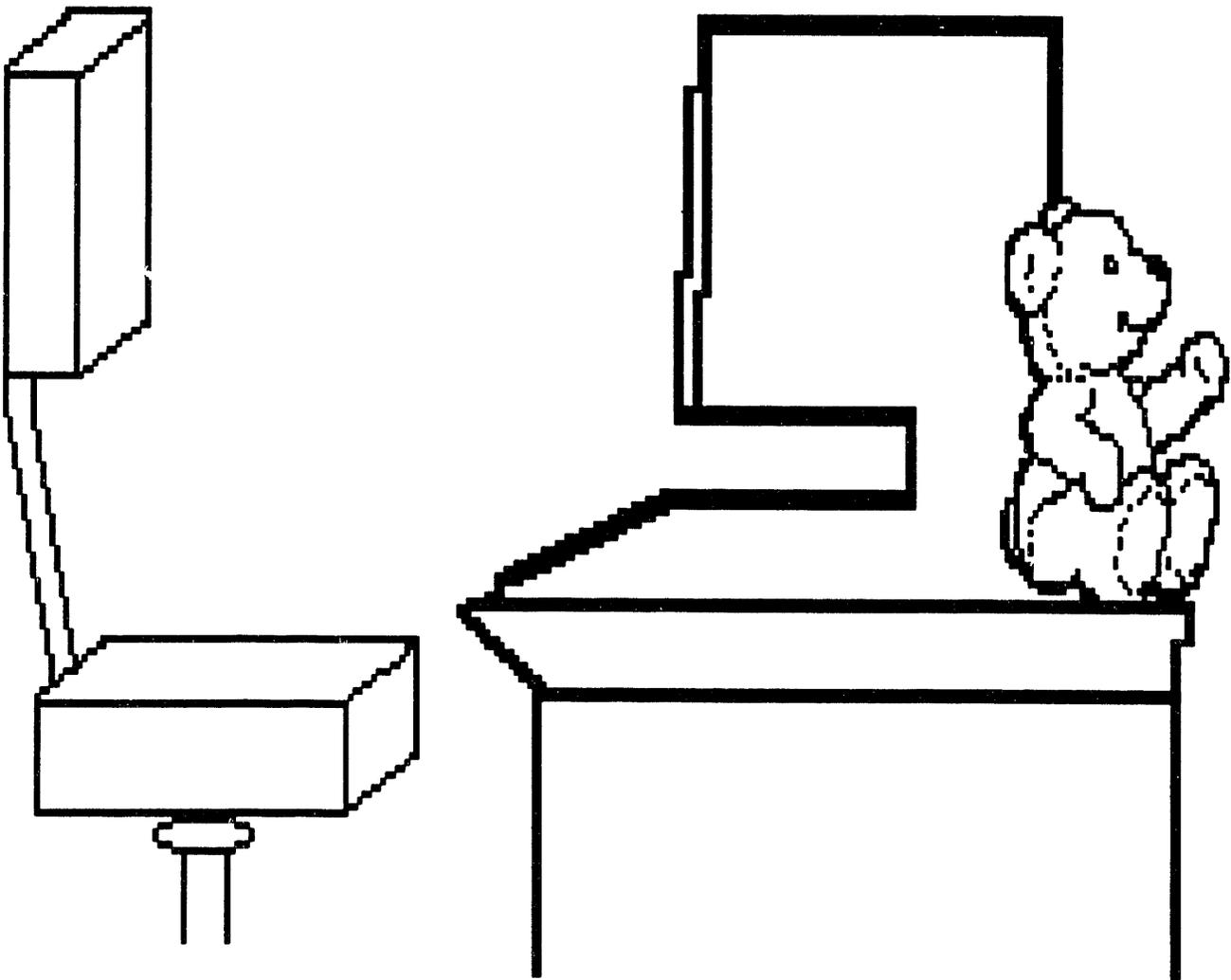
© The Regents of the University of California 1993

We have a lot of
computers at
Lawrence Livermore
National Laboratory.





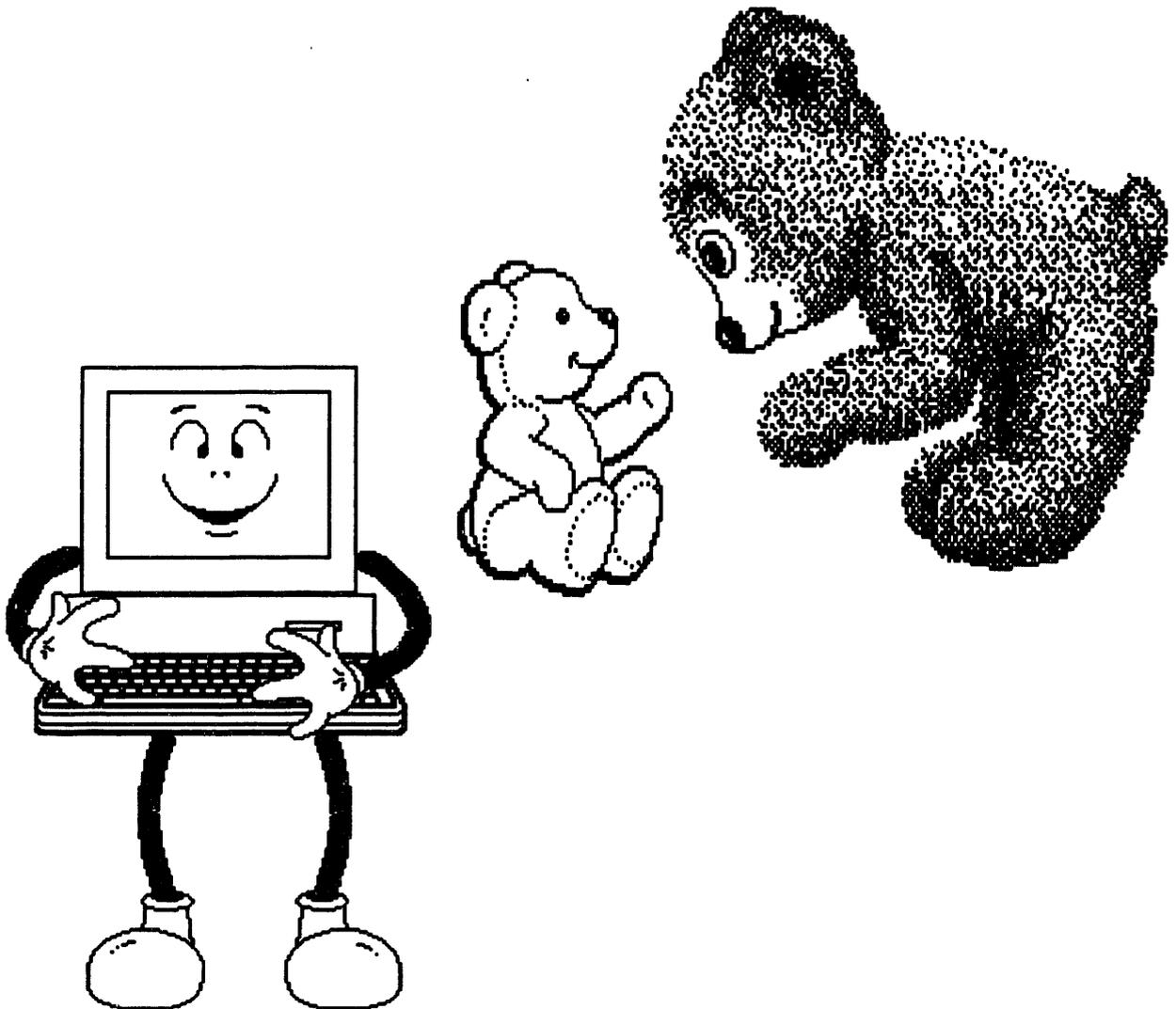
YOU can use
computers too.



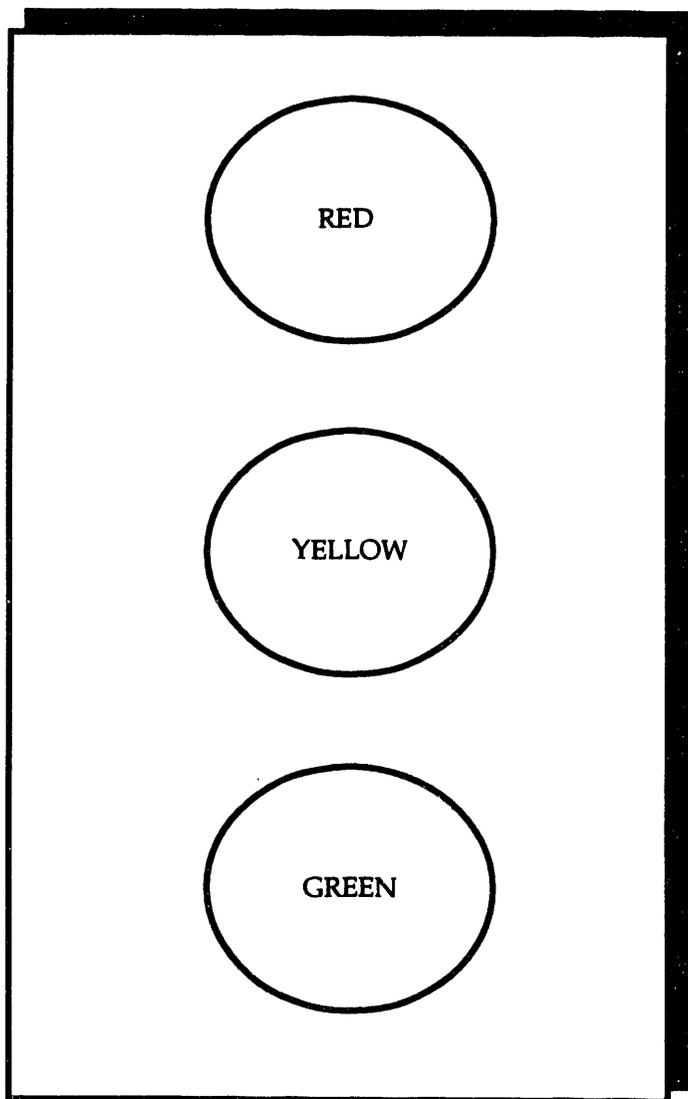
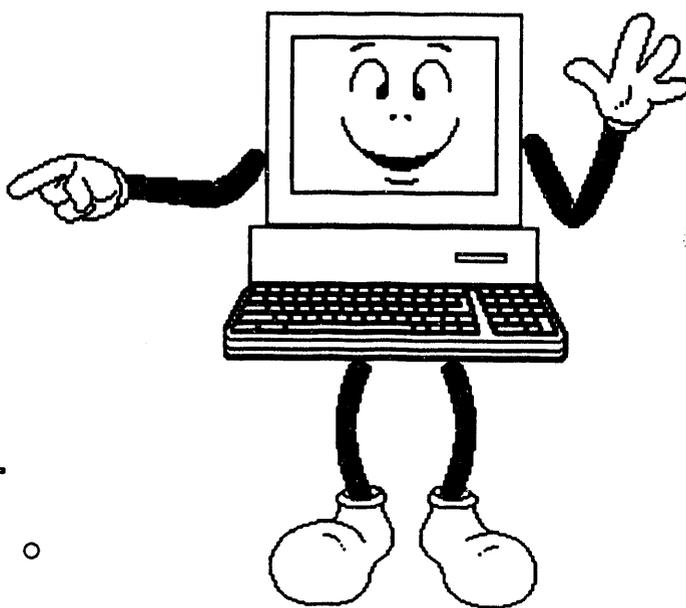
Draw a picture of yourself.

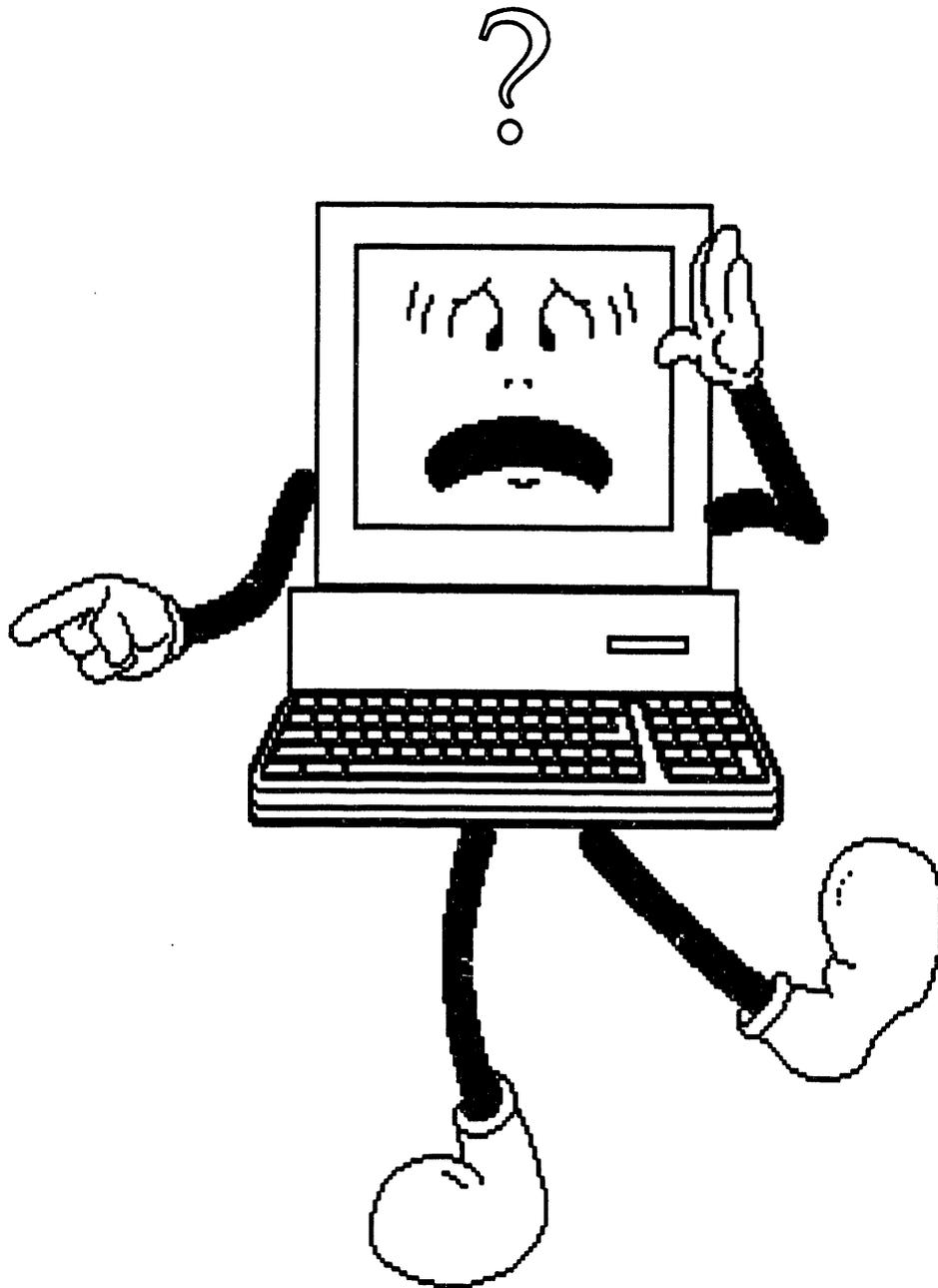


Computers are
your friends!
Take good care
of them.

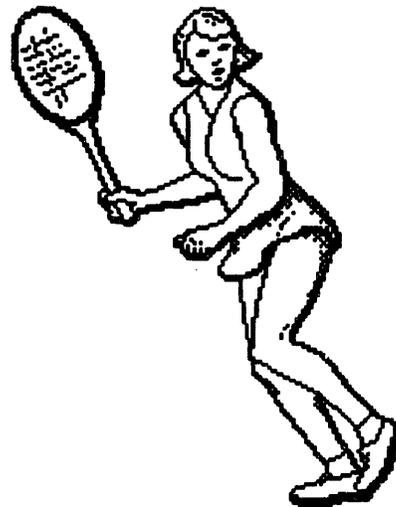
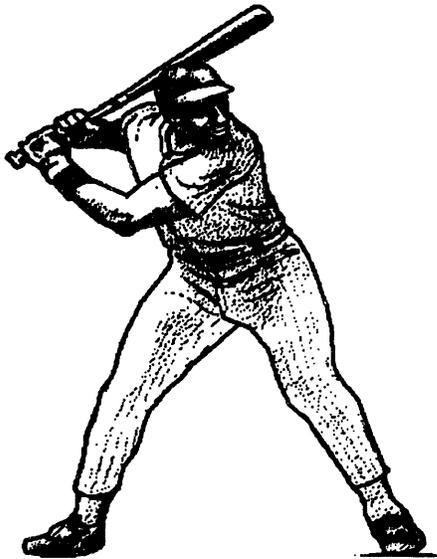
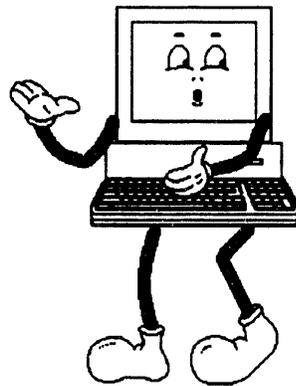
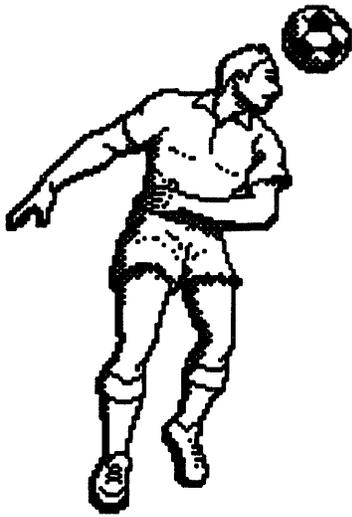


STOP,
LOOK,
and
LISTEN.

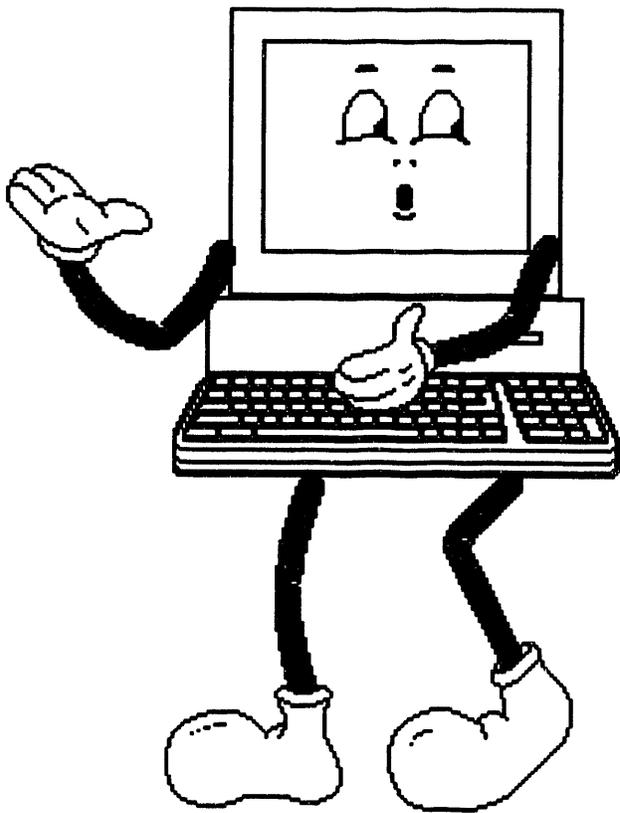
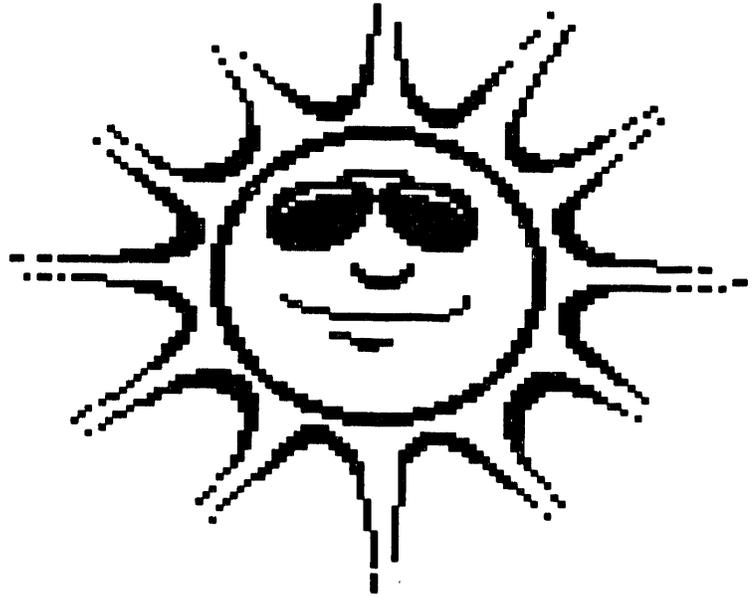




If something goes
wrong with your
computer, stop and ask a
grown-up to help.

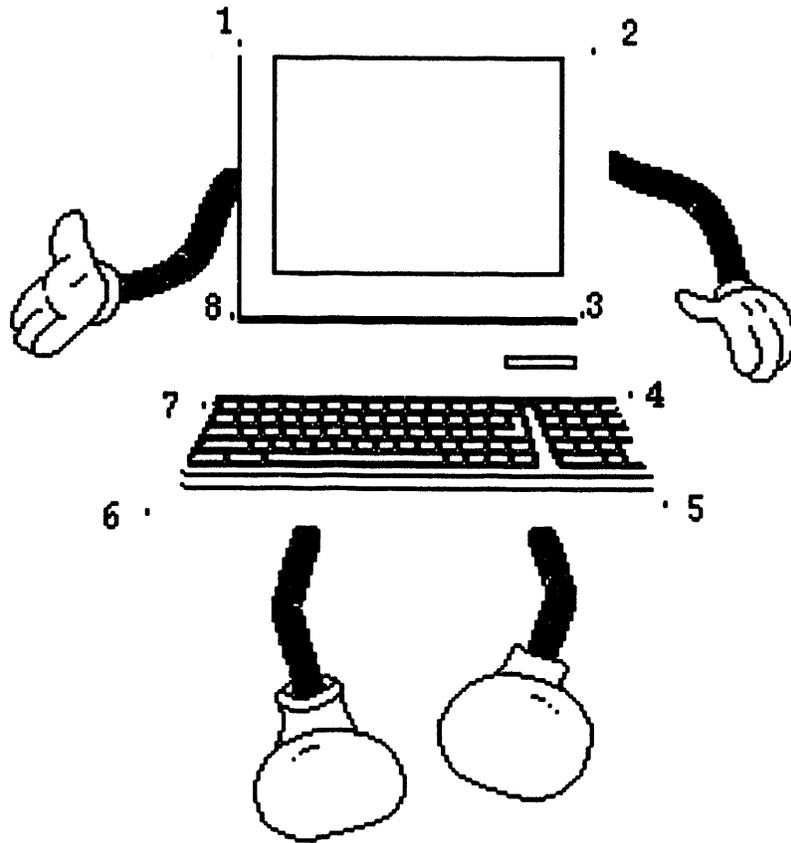


Be careful when
playing near a computer.

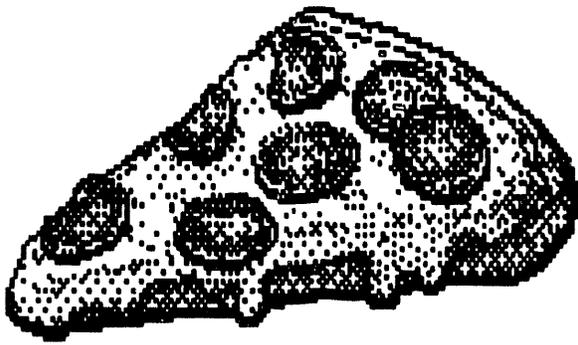


Chip says, "Please keep me away from hot things!"

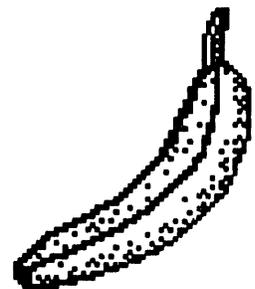
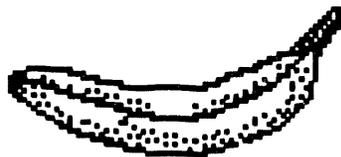
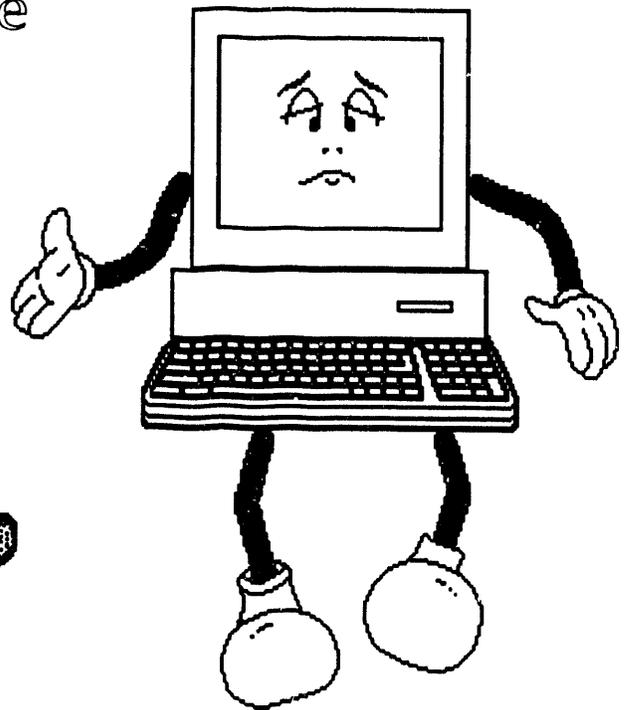
Oh, dear me
I'm quite undone.
Connect the dots
and have some fun!



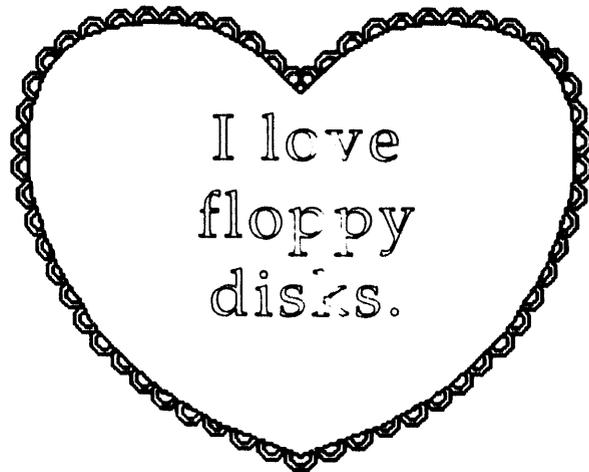
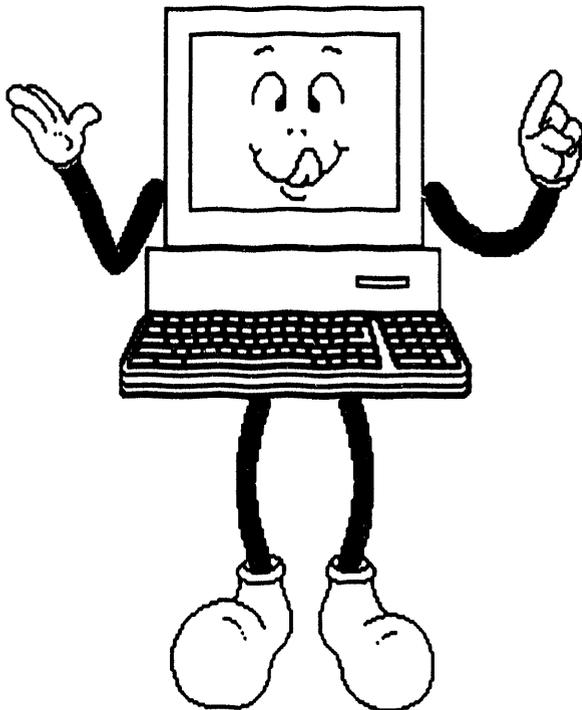
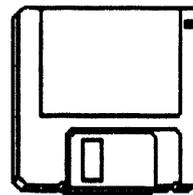
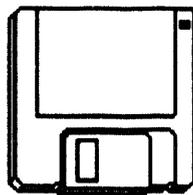
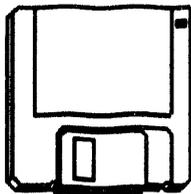
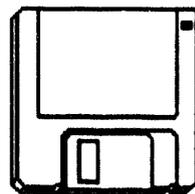
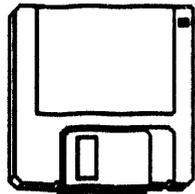
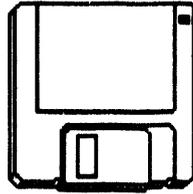
After you've connected
the dots, please draw
me a happy face.



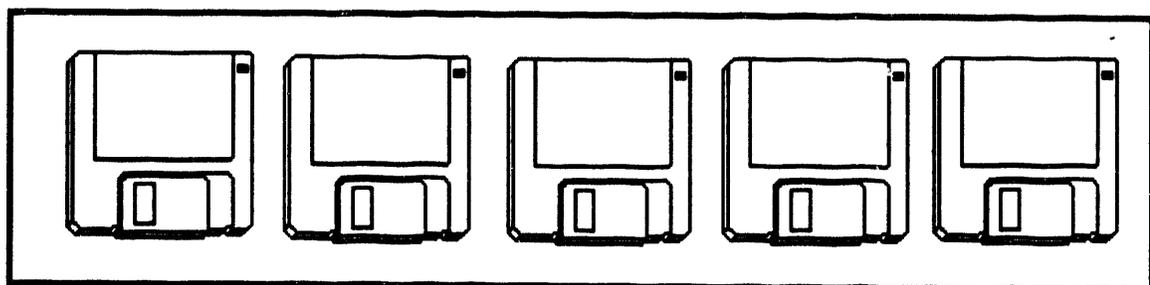
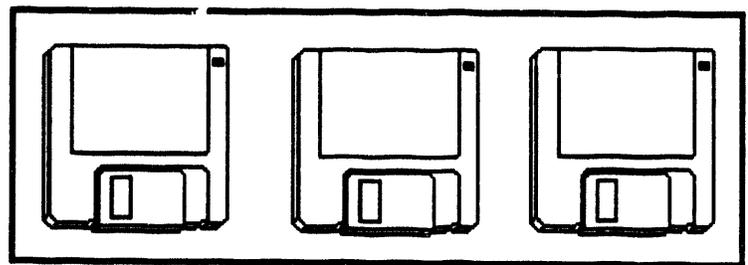
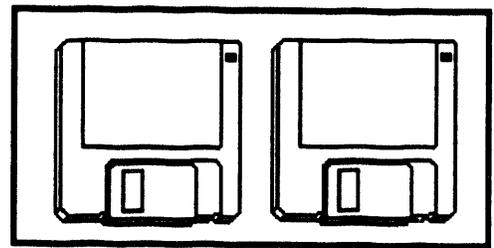
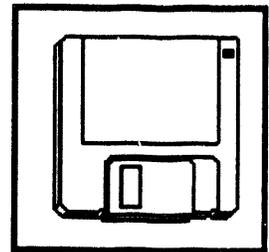
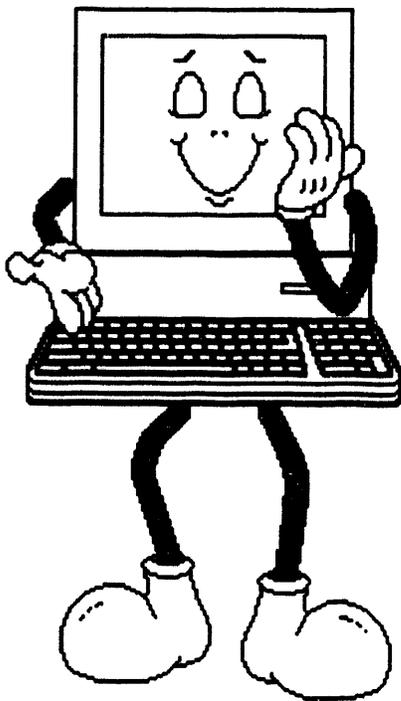
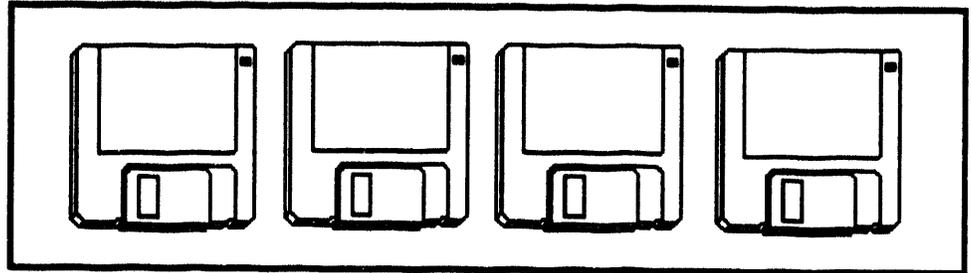
Please eat and drink
away from me. I like
floppy disks, not
people foods.

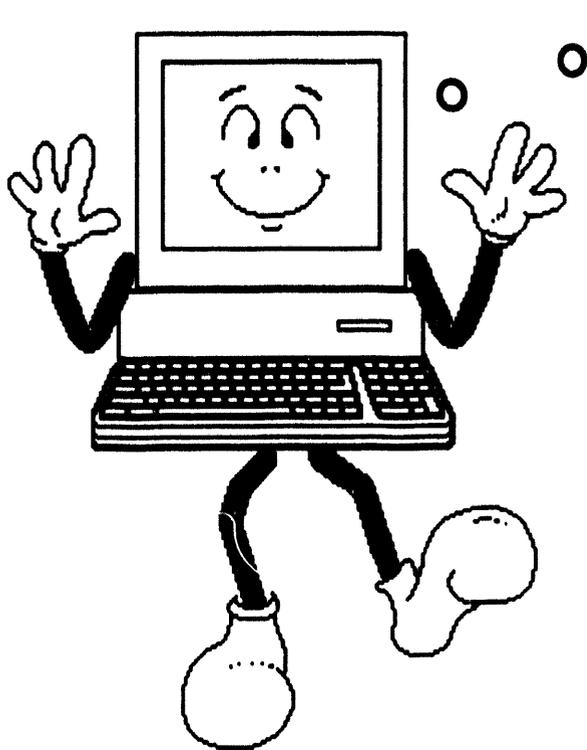


Color the floppy disks
one by one,
and let's have some
computer fun.



Draw a line from Chip to the
box with 5 floppy disks.





Good bye now from
Lawrence Livermore
National Laboratory.

We're glad we could come to
your school to help you learn
about using computers safely.

The LLNL Computer Security organization is part of the Laboratory's Computation Organization.
Chip's Coloring Book by Gale Warshawsky and Lonnie Moore.

© The Regents of the University of California 1993

The following CHIP SAYS cartoons are copyrighted to
Gale Warshawsky and Lonnie Moore, 1994.

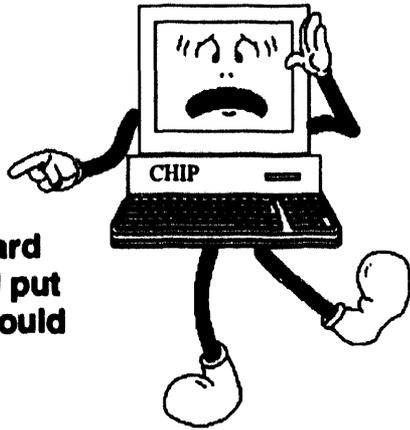
Acknowledgement of Government Sponsorship and License Rights

NOTICE: The Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, and perform publicly and display publicly. Beginning five (5) years after March 31, 1994, the Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, distribute copies to the public, perform publicly and display publicly, and to permit others to do so.

NEITHER THE UNITED STATES NOR THE UNITED STATES DEPARTMENT OF ENERGY, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS.

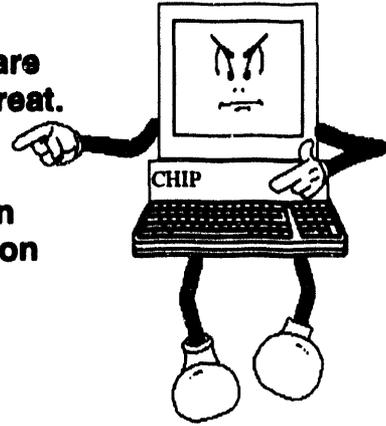
CHIP SAYS © 1994

Don't download software from a Bulletin Board Service and put it on me. I could get a virus that way!



CHIP SAYS © 1994

New viruses are a constant threat. Be sure you use the most recent version virus protection software to protect me!



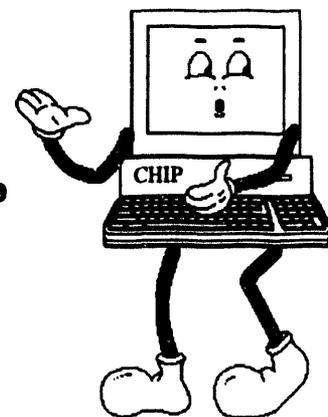
CHIP SAYS © 1994

Do backups on a regularly scheduled basis.



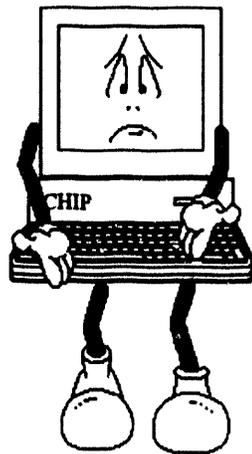
CHIP SAYS © 1994

When was the last time you did backups?



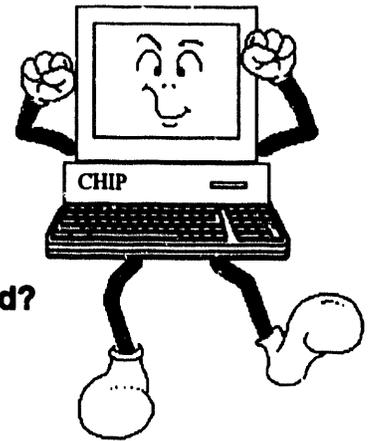
CHIP SAYS © 1994

Have you
marked your
hardware and
software with
approved
labels?



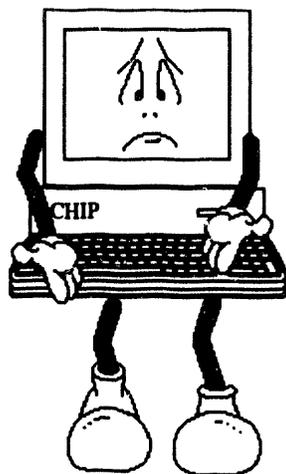
CHIP SAYS © 1994

Don't get
punchy!
When was
the last time
you changed
your password?



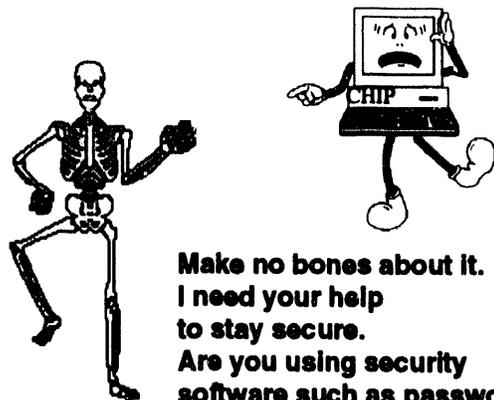
CHIP SAYS © 1994

DON'T put
illegal
software
on me!
Software
Piracy is
against
the law.
Please
read your
software
licensing
agreements.



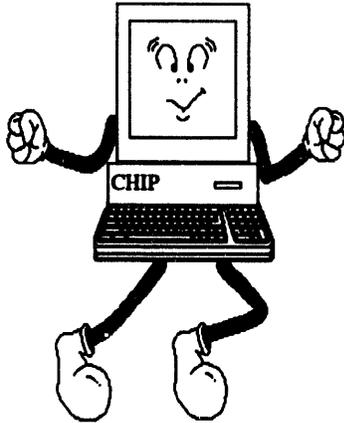
CHIP SAYS © 1994

Make no bones about it.
I need your help
to stay secure.
Are you using security
software such as password
protection screen savers
and virus checking software
on me?



CHIP SAYS © 1994

When escorting a non-cleared person, make sure YOU stay with them at all times. Make sure they do not have any unauthorized access to information.



CHIP SAYS © 1994

Create good passwords:

DON'T use any personal information.

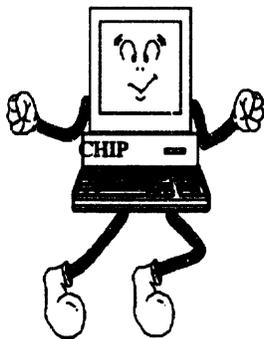
DON'T use words found in any dictionary.

DO mix up letters and numbers to make a word-phrase that you can remember.

DON'T make your password so hard to remember that you have to write it down.

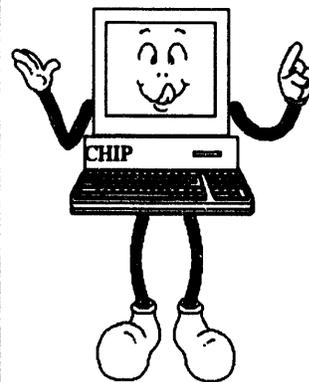


CHIP SAYS © 1994



Have you watched the DOE video, *Introduction to the Unclassified Computer Security Program*? Contact your CPPC to request a copy of this video.

CHIP SAYS © 1994

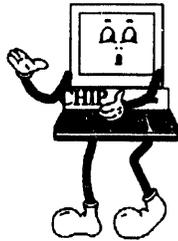


Floppies with viruses taste good too. I need your help so I won't get sick! Use virus checking software to scan your floppy disks.

CHIP SAYS © 1994



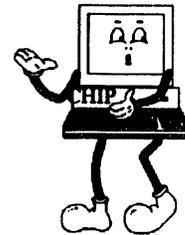
IT'S 11 O'CLOCK!



**DO YOU KNOW
WHAT YOUR
COMPUTER IS DOING?**

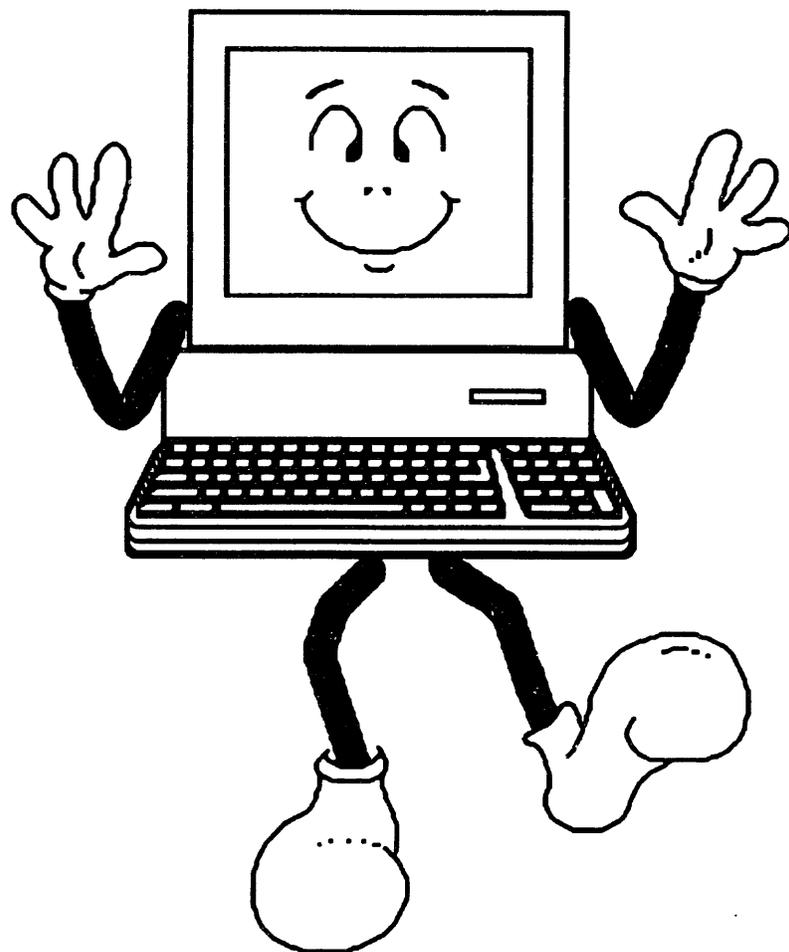
CHIP SAYS © 1994

**Please don't leave me
active and vulnerable...**



**when you leave,
lock-up and logout.
Keep our Information secure.**

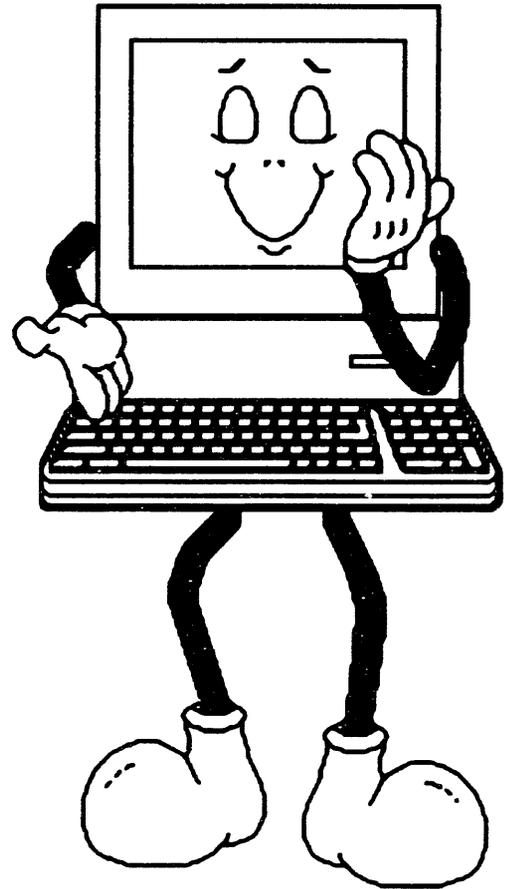
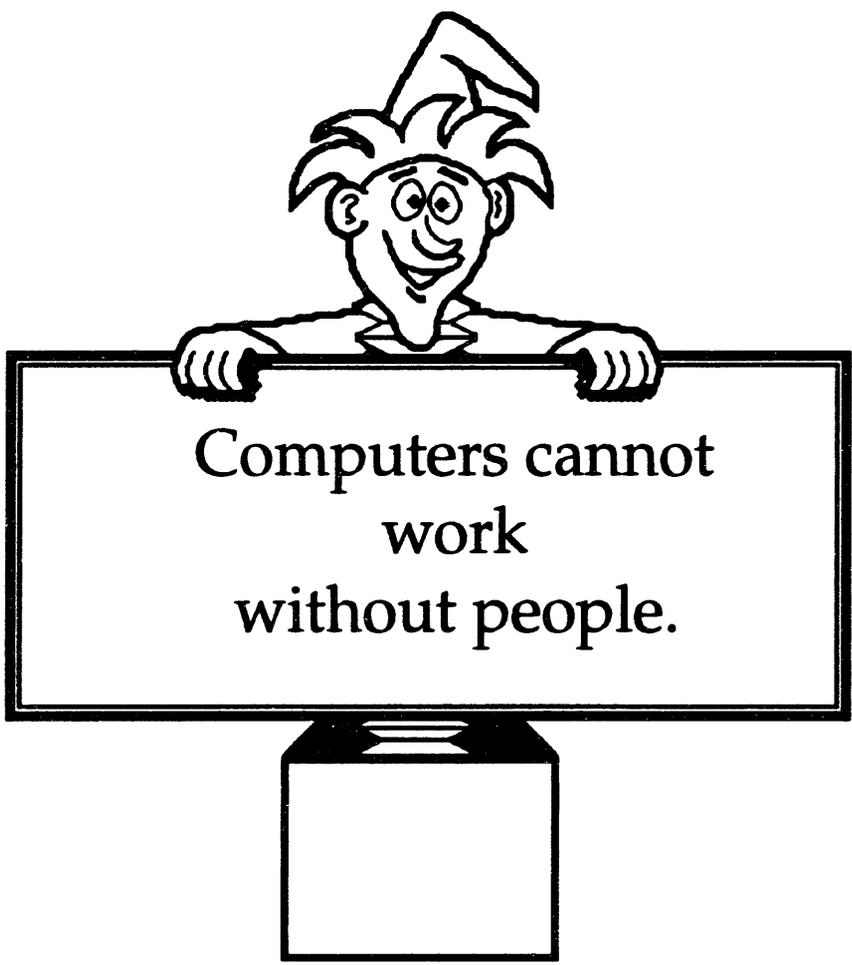
Hi. I'm Chip.



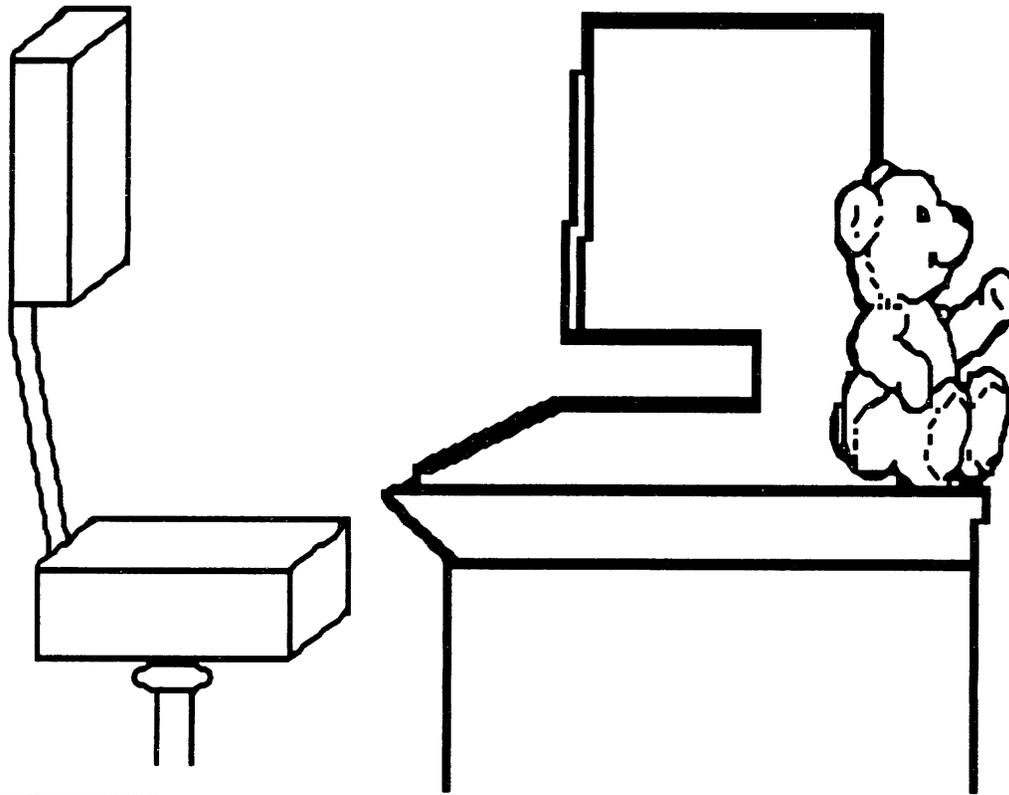
Lawrence Livermore National Laboratory Transparencies UCRL-MI-113637

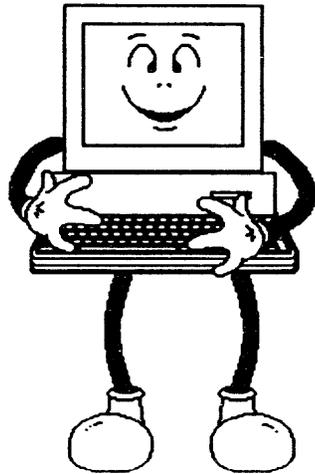
© The Regents of the University of California 1993

UCRL-MI-113637
APPENDIX 5



You can use computers too.



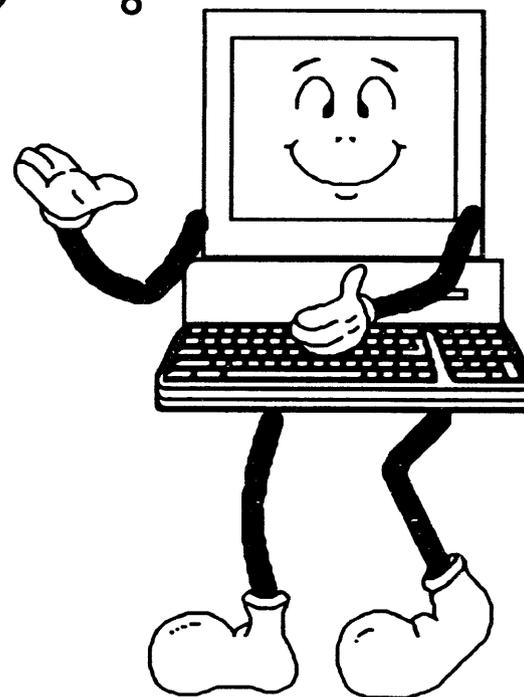


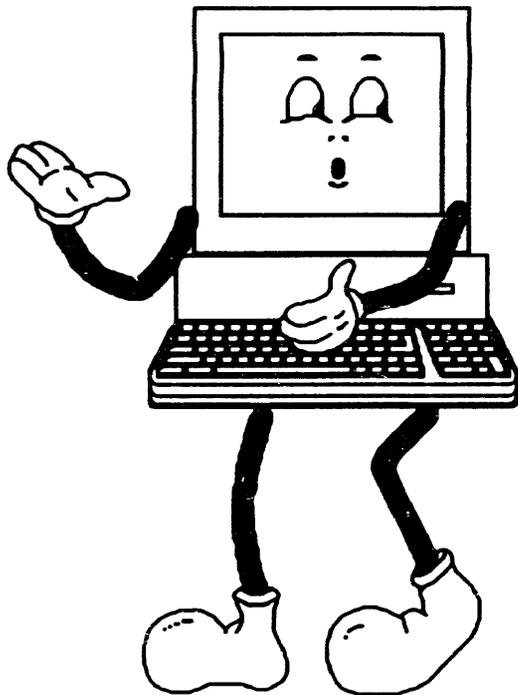
**Computers are
your friends!**

**Take good care
of them.**



**How can we
protect our information?**

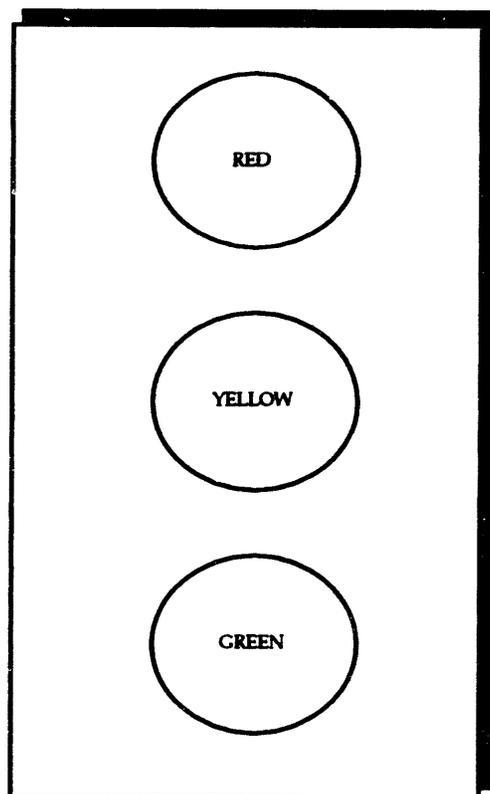


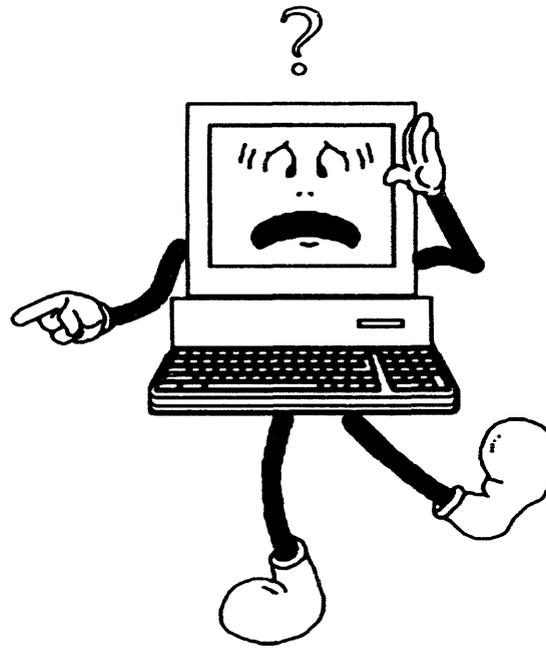


What is a password?

**How can a password
help you to protect
Chip?**

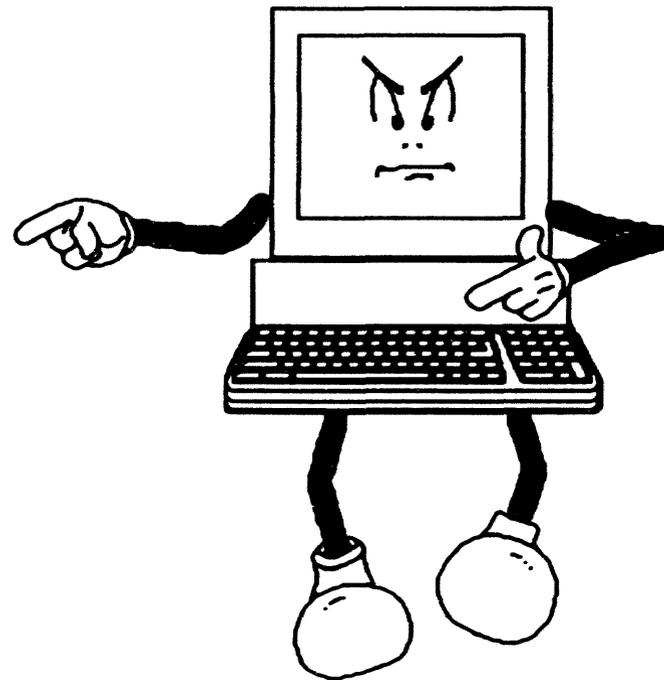
STOP, LOOK, AND LISTEN.

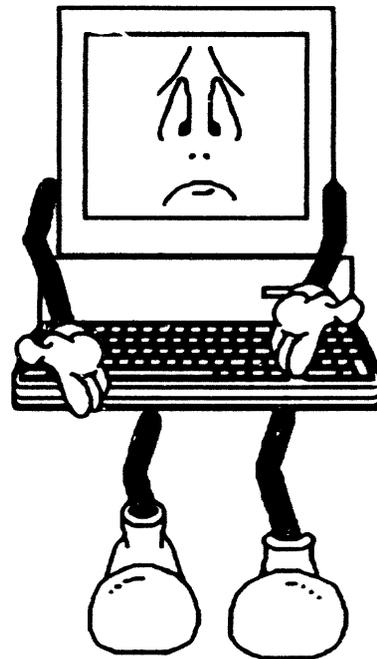




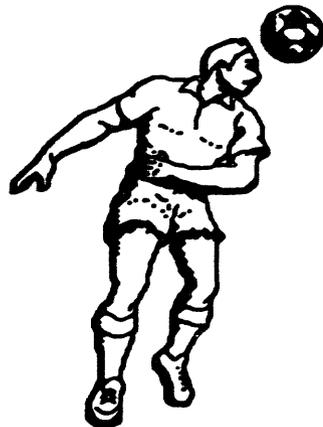
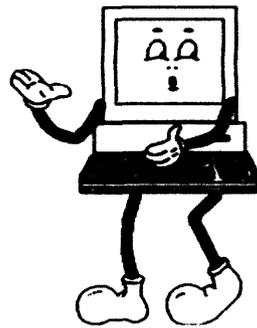
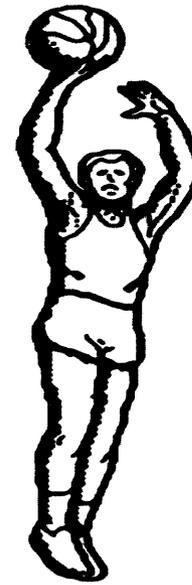
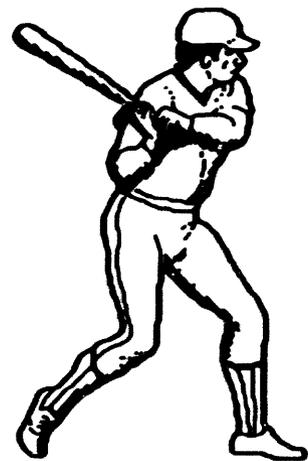
**If something goes
wrong with your
computer, stop and ask a
grown-up to help.**

**Sometimes people do bad things
to computers and information.**

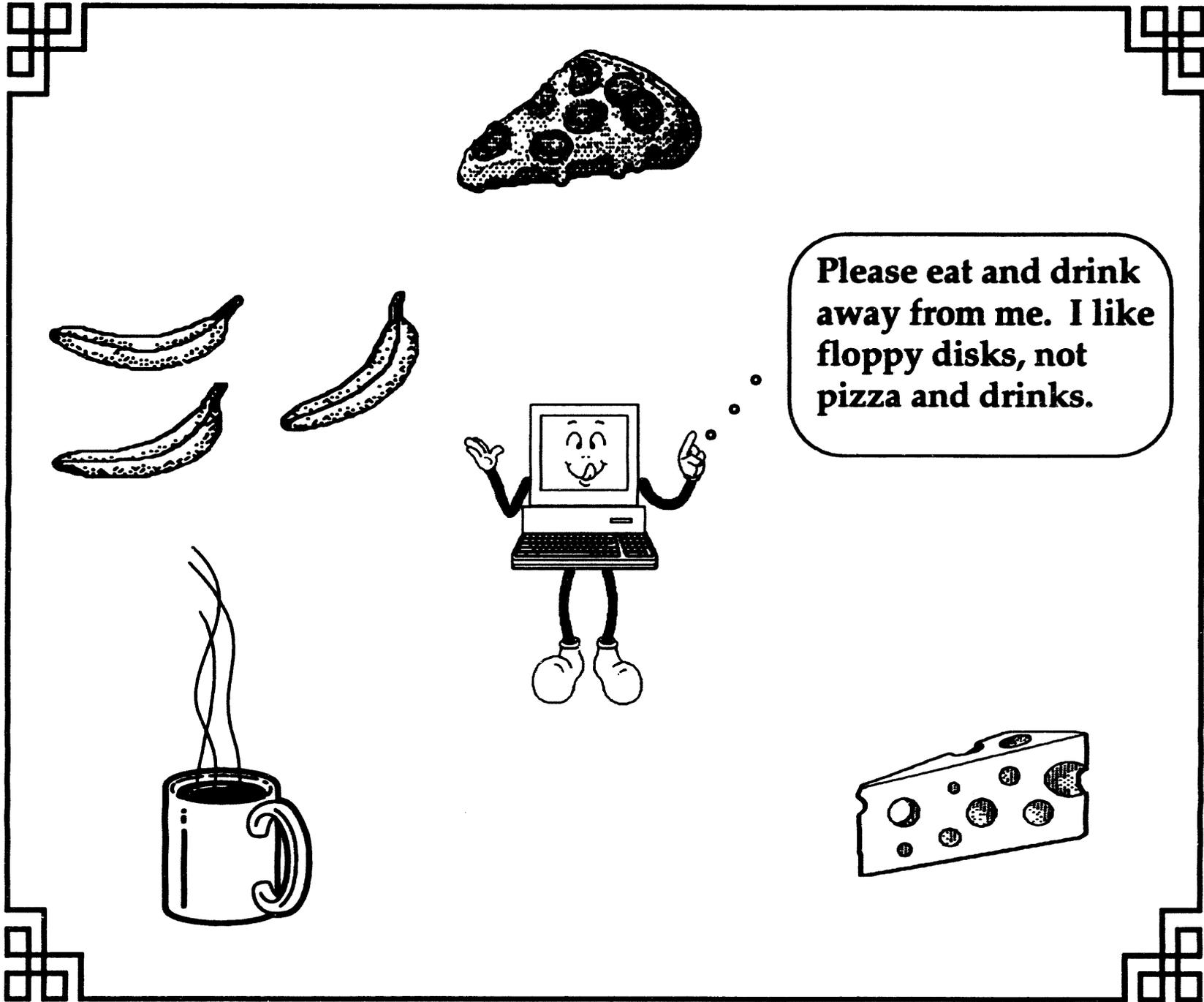




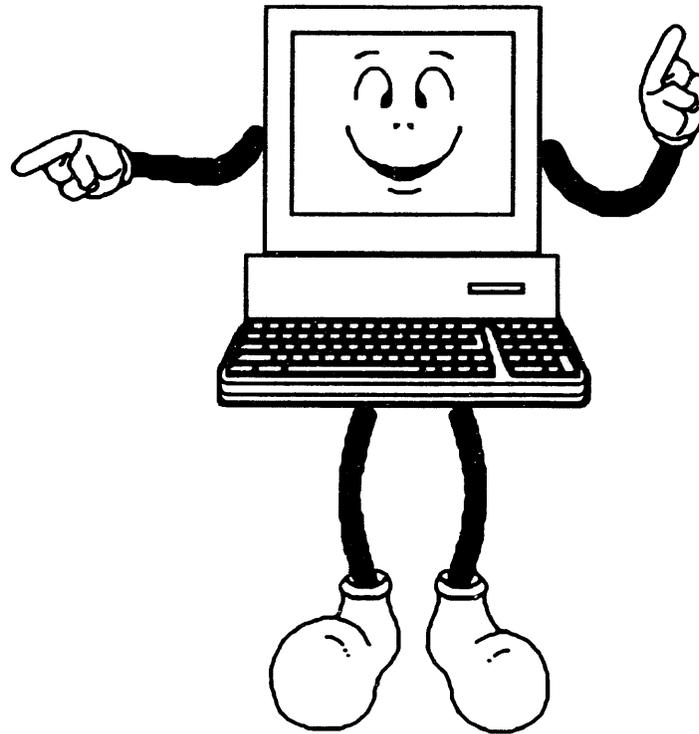
What things did Dirty Dan do that were not very nice to Gooseberry's information on the computer?



Be careful when playing near a computer.



Chip Says:



EVERYBODY needs computer security!

Acknowledgment of Government Sponsorship and License Rights

NOTICE: The Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, and perform publicly and display publicly. Beginning five (5) years after March 31, 1994, the Government is granted for itself and others acting on its behalf a paid-up, nonexclusive, irrevocable worldwide license in this data to reproduce, prepare derivative works, distribute copies to the public, perform publicly and display publicly, and to permit others to do so.

NEITHER THE UNITED STATES NOR THE UNITED STATES DEPARTMENT OF ENERGY, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS.

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-ENG-48. UCRL-MI-113637.

DATE

FILMED

7/5/94

END

