

**INSPECTOR
GENERAL**

U.S. Agency For International Development
Office of Security
Washington, D.C. 20523

WHAT IS COMPUTER SECURITY?

It's protecting your organization's information and equipment from damage or loss.

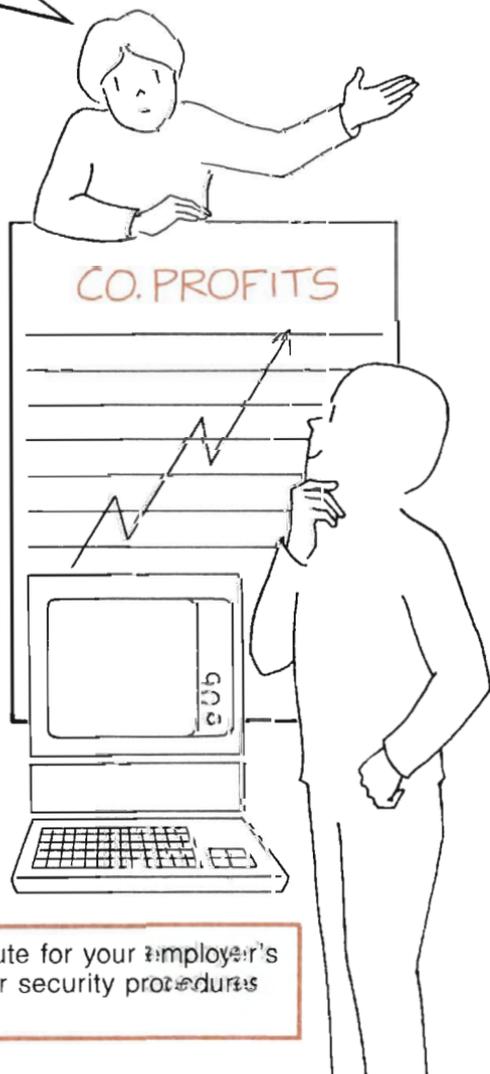
COMPUTER TECHNOLOGY

has made a big difference in the way organizations work. Main frames, minicomputers and microcomputers all need protection.

COMPUTER SECURITY

means protecting your organization's computer-based resources, including:

- hardware -- the physical parts of the computer itself
- software -- operating systems and programs that tell the computer what to do
- data -- information used in a program
- media -- magnetic devices that store data and programs.



This booklet is not a substitute for your employer's or any government computer security procedures and policies.





**WHY
LEARN ABOUT
IT?**

Because computer security is every employee's responsibility!

**YOUR ORGANIZATION
RELIES ON HONEST,
CAREFUL EMPLOYEES**

like you to keep security in mind at all times.

Protecting computer-based resources is one of the most important things you can do for your organization!

Learn more...

COMPUTER-BASED INFORMATION IS VALUABLE!

For example, you may need to protect:

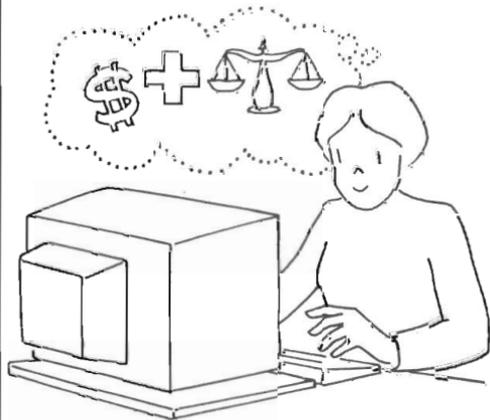
CUSTOMER OR PATIENT INFORMATION,

such as historical data, medical records or client lists.



EMPLOYEE INFORMATION,

such as personnel files, payroll data, or legal or medical records.



TRADE SECRETS,

such as product designs, marketing plans, price changes or manufacturing information.



GOVERNMENT INFORMATION,

including documents that may be vital to our national security!



AND, COMPUTERS ARE VULNERABLE

For example, data can be jeopardized through:

ERRORS

Everyone makes mistakes, but mistakes can be costly when they affect computer-based resources.



MISUSE OF THE SYSTEM

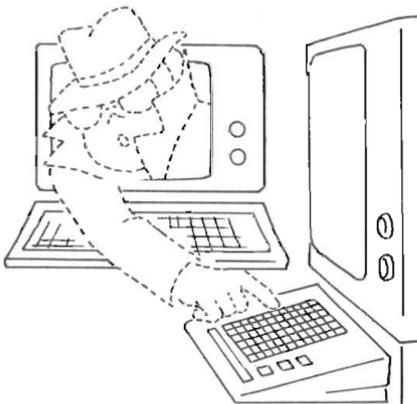
Data can be threatened by an "insider" who:

- doesn't follow proper procedures
- uses data for illegal purposes
- installs a computer virus (see page 14).



INDUSTRIAL "SPYING"

"Hackers" can use networking systems to steal trade secrets or other information.



NATURAL HAZARDS

Computer-based resources can be lost or damaged by:

- fire
- smoke
- static electricity
- extreme temperatures
- humidity
- magnetic forces.

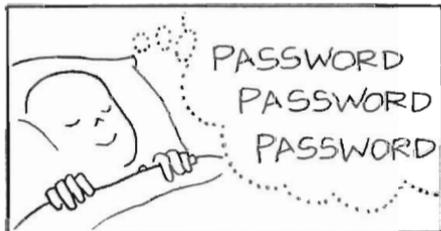
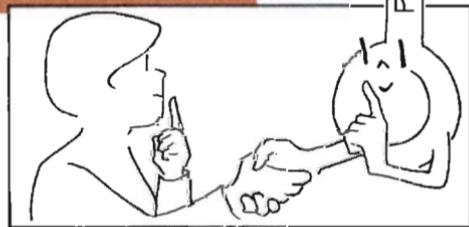
Learn to practice computer security...

YOUR PASSWORD IS YOUR KEY

to your organization's computer system.
Use it properly -- and protect it!

KEEP IT CONFIDENTIAL

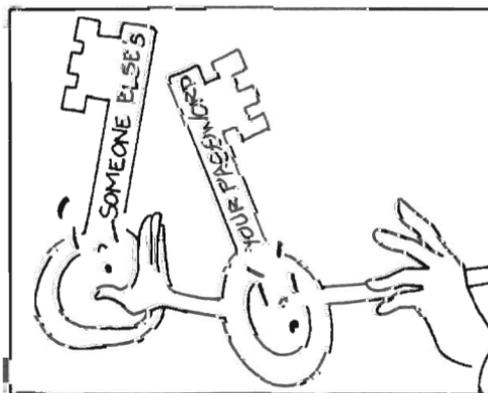
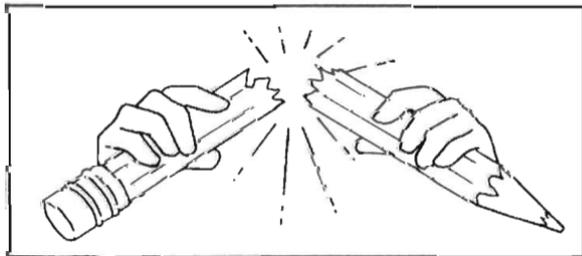
— it's your business
and no one else's!



MEMORIZE IT

DON'T WRITE IT DOWN

or store it in the system.



**DON'T USE
ANYONE ELSE'S**
password.

CHANGE IT PERIODICALLY,

following your organization's procedures.

MAKE SURE IT'S THE PROPER LENGTH,

according to company
guidelines.

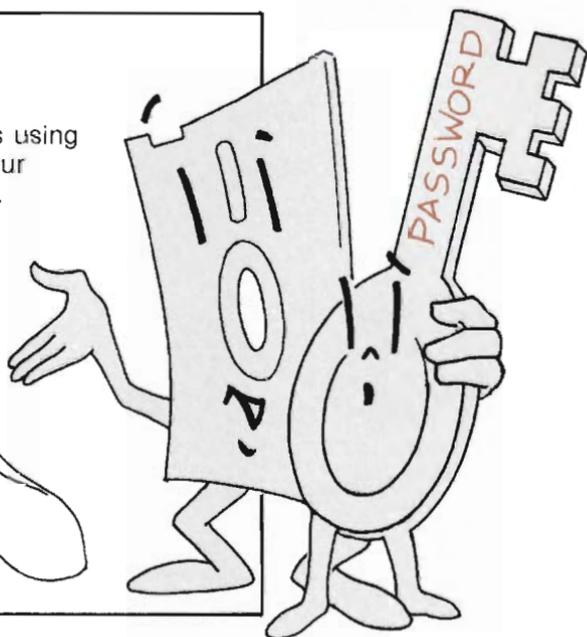
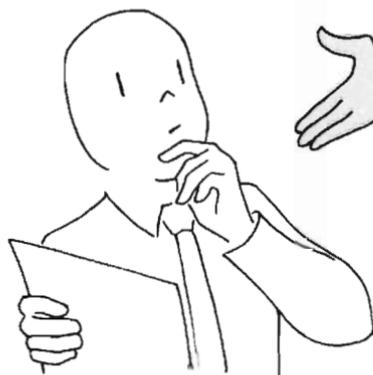


CHOOSE ONE THAT'S UNIQUE

– not one that will be easily
guessed, such as your birth-
day, favorite sport or spouse's
name.

NOTIFY YOUR SUPERVISOR

if you think someone is using
your password, or if your
password isn't working.



LEARN THE BASICS

Make these computer security rules a routine part of your job:

ACCESS ONLY THE DATA YOU NEED

in order to do your job.

USE A KEYBOARD OR SYSTEM LOCK, if available.

if available.

DON'T LEAVE THE COMPUTER ON OR UNATTENDED

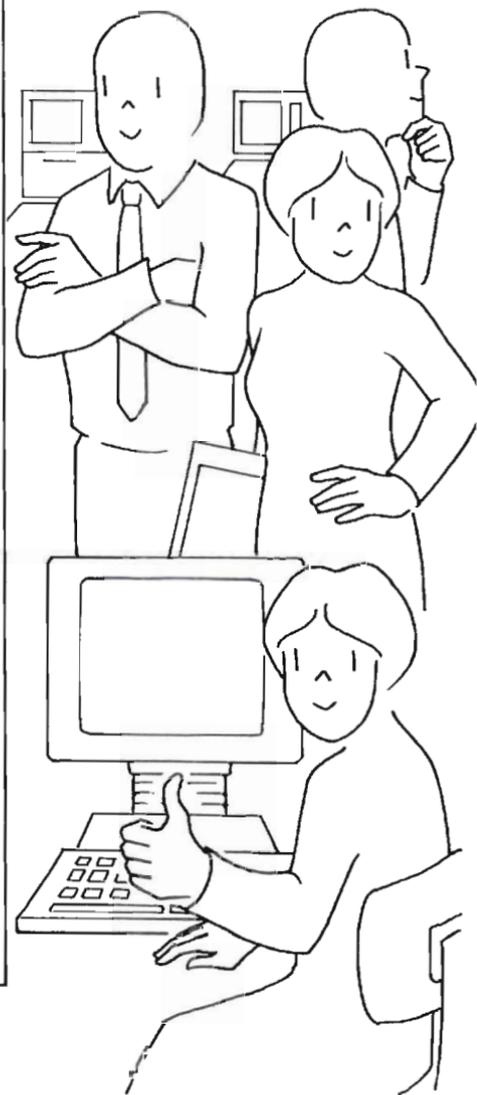
– always log off if you have to leave – even for a moment.

PROPERLY DISPOSE OF UNNEEDED DATA

– make sure that information you don't need is deleted permanently.

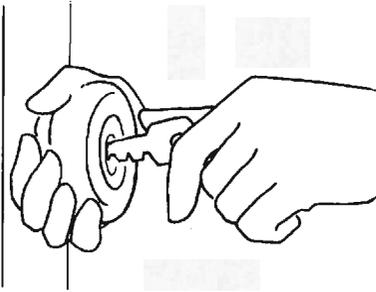
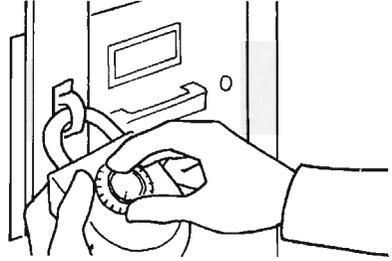
DON'T LEAVE SENSITIVE INFORMATION

in your PC or terminal.



**LOCK UP
OR DESTROY
PRINTOUTS,**

and other written information properly. (Don't throw sensitive information in the waste-basket.)



**REMEMBER TO
LOCK THE ROOM**

where your PC or terminal is located, to keep it safe.

**GET YOUR
SUPERVISOR'S
PERMISSION**

before you change any software program.

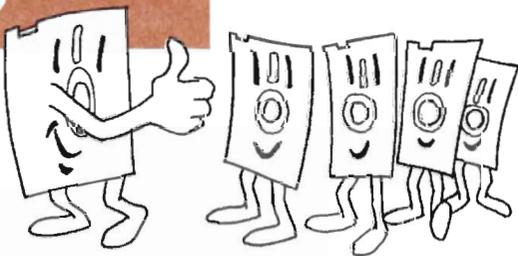


**Remember -- you are
an important part of
your organization's
security team!**

MORE TIPS

BACK UP ALL DATA

periodically on diskettes or tape. This is very important!

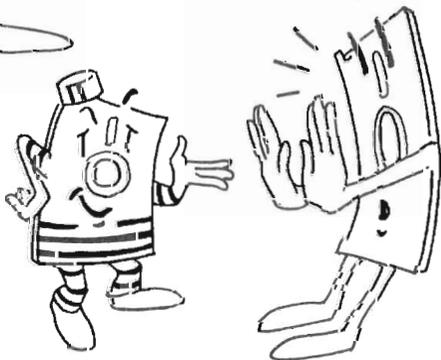
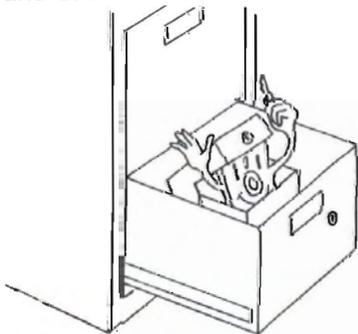


DON'T SMOKE, EAT OR DRINK

while using the computer system
– any spills could damage it.

DON'T USE UNAUTHORIZED SOFTWARE

– it could damage programs
and data.

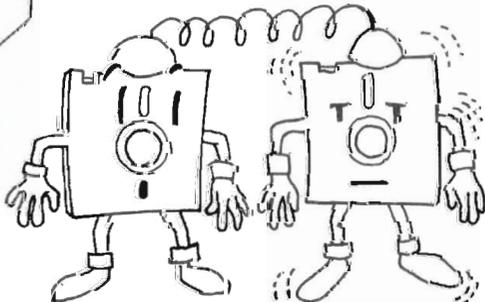


PROTECT SOFTWARE

– don't leave it where it
could be altered or stolen.

DON'T DUPLICATE SOFTWARE

or violate copyrights in
any way.



If you notice any unusual activity on your computer, or if you make any mistakes, contact your supervisor promptly.

CARE PROPERLY FOR DISKETTES

to ensure that important information is available when you need it.

LABEL ALL DISKETTES,

especially if they contain sensitive data.

KEEP DISKETTES SAFE FROM HAZARDS,

such as electrical or magnetic forces, dust, heat and liquids.

REMOVE DISKETTES FROM THE COMPUTER

when they're not in use.

PROPERLY PACKAGE AND TRANSPORT DISKETTES

and other resources (such as printouts or portable computers). Follow company security procedures if transporting sensitive information.

STORE DISKETTES OR TAPES

with other critical information in a secure location.

Ask your supervisor, if you have questions regarding any procedure.



REPORT ALL VIOLATIONS

Become the "eyes and ears" of your workplace!

Violations may include:

USING SOMEONE ELSE'S PASSWORD

PERSONAL USE OF COMPUTERS

– your organization's computers are for official use only

CHANGING OR COPYING DATA

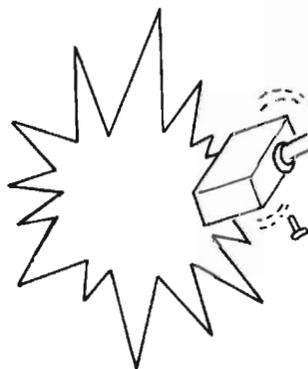
without permission

DAMAGING

or destroying hardware or software

DELIBERATELY SLOWING THE PROCESSES

of the computer system





VIOLATING FEDERAL LAWS

while using a computer or terminal belonging to your organization

THEFT

of hardware or software

DELIBERATELY ERASING DATA

that should not be deleted

LEAVING EQUIPMENT UNATTENDED,

or computer rooms unlocked when no one is inside

Stay alert -- it's one of the best ways to practice computer security!

SOME QUESTIONS AND ANSWERS

Are there any laws protecting computer-based data?



Yes. The Computer Security Act of 1987 helps protect federal computer-based resources. It calls for users of federal computer systems to be trained in computer security. Also, the Computer Fraud and Abuse Act makes it illegal to access a federal computer without authorization.

What is a computer virus?



It's a dangerous type of program introduced into a computer system. It can spread to other systems, causing:

- loss or ruin of computer-based data
- destruction of hardware and software
- lost productivity.

How can I protect against viruses?

Follow basic security rules, such as:

- Make sure your supervisor has reviewed and authorized any software you use.
- Don't download software from bulletin boards.
- Use only media from a reputable source.
- Promptly report anything unusual to your supervisor.

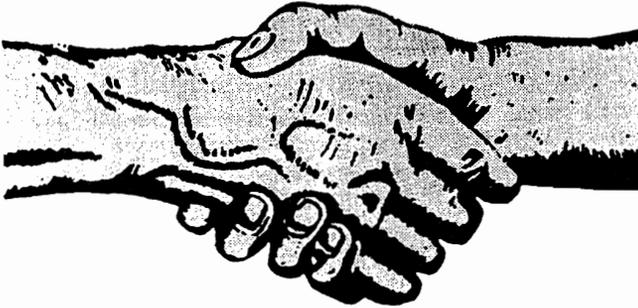
Soo--

PRACTICE COMPUTER SECURITY!

- ✓ **UNDERSTAND THE REASONS** for security.
- ✓ **PROTECT YOUR PASSWORD.**
- ✓ **FOLLOW SECURITY RULES** at all times.
- ✓ **REPORT VIOLATIONS** and any problems immediately.



Your organization's security is in your hands!



UNITED STATES OF AMERICA



Printed on Recycled Paper.