InfoSec Update

Overview of 2000

Technical Vulnerabilities

David Kennedy CISSP

Director of Research Services

<david.kennedy@acm.org>

Agenda

- Good News
- Bad News
  - DDoS--No excuses, we had plenty of warning
  - ILOVEYOU-- No excuses, we had plenty of warning
  - Pervasive Scanning
  - 2000--The Year of the Buffer Overflow (n_{th} iteration)

Agenda (cont)

- It may work, but it doesn't *work*
- Trojans and Back Doors
- Nightmares
- KISS

Sources

- Bugtraq
- NTBugtraq
- FIRST Member Advisories
- Vendor Advisories
- 104 Other Security and UG Mailing Lists
- USENET
- ~1400 ‘Net Sites and BBS

http://www.forbes.com/tool/html/98/jul/0703/side1.htm

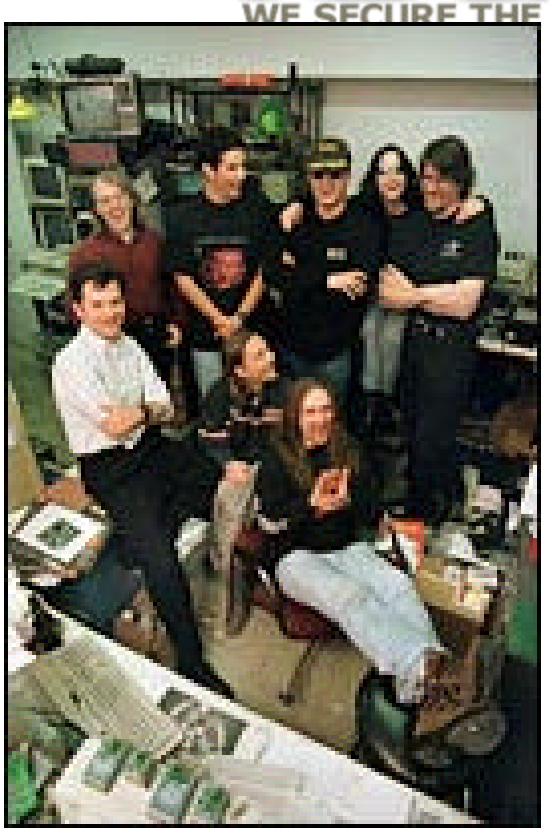
Wall Street Journal 9/30/99, page B21

Good News

- Vendors are getting proficient at making security notifications
  (Practice makes perfect?)
- Source auditing for security is paying off.
- Job security outlook continues to be rather bright

Bad News

- DDoS--We Had Plenty of Warning
- ILOVEYOU--We Had Plenty of Warning
- Scans
- Buffer overflows continue



l0pht

ILOVEYOU--Talismans

- Happy99 a.k.a W32/SKA.exe (1/99)
- Melissa Macro.W97.Melissa (3/99)
- VBS.Freelink (7/99)
- Barok (same author(s)) (9/99)
- Bubbleboy I-Worm.BubbleBoy (11/99)

Scans

NMAP

DNS Queries

SNMP Walk

Whois and NSLookup

Rootshell & Packetstorm

SATAN

stobe

mscan

Nessus

SAINT

Asmodeus

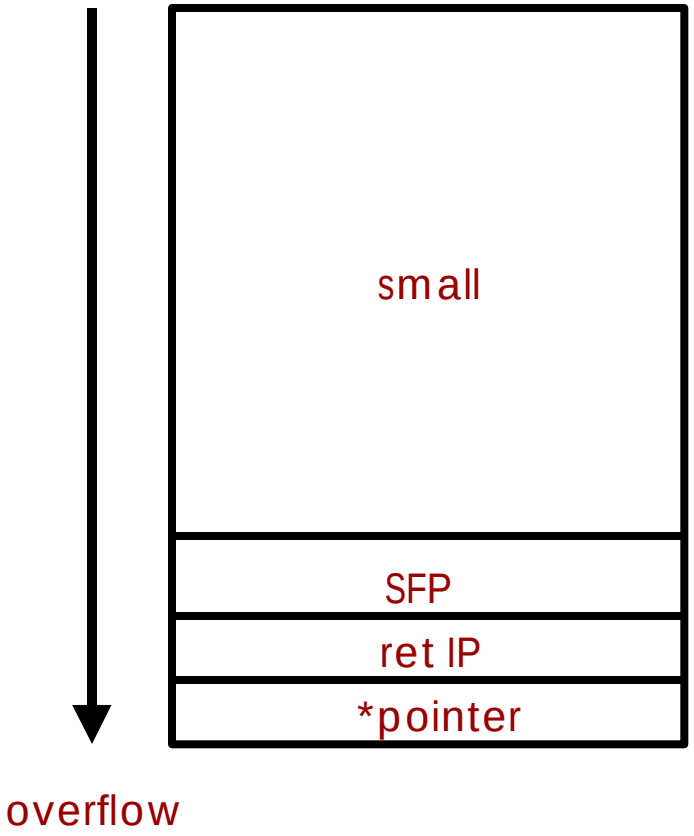
Internet Probe Droid

Warez

- ISS
- CyberCop
- HackerShield
- Security Analyzer

2000A.D.--The Year of the Buffer Overflow (Again)

- Phrack 49 & Fall '96 *2600* Article
- Stackguard
- Languages

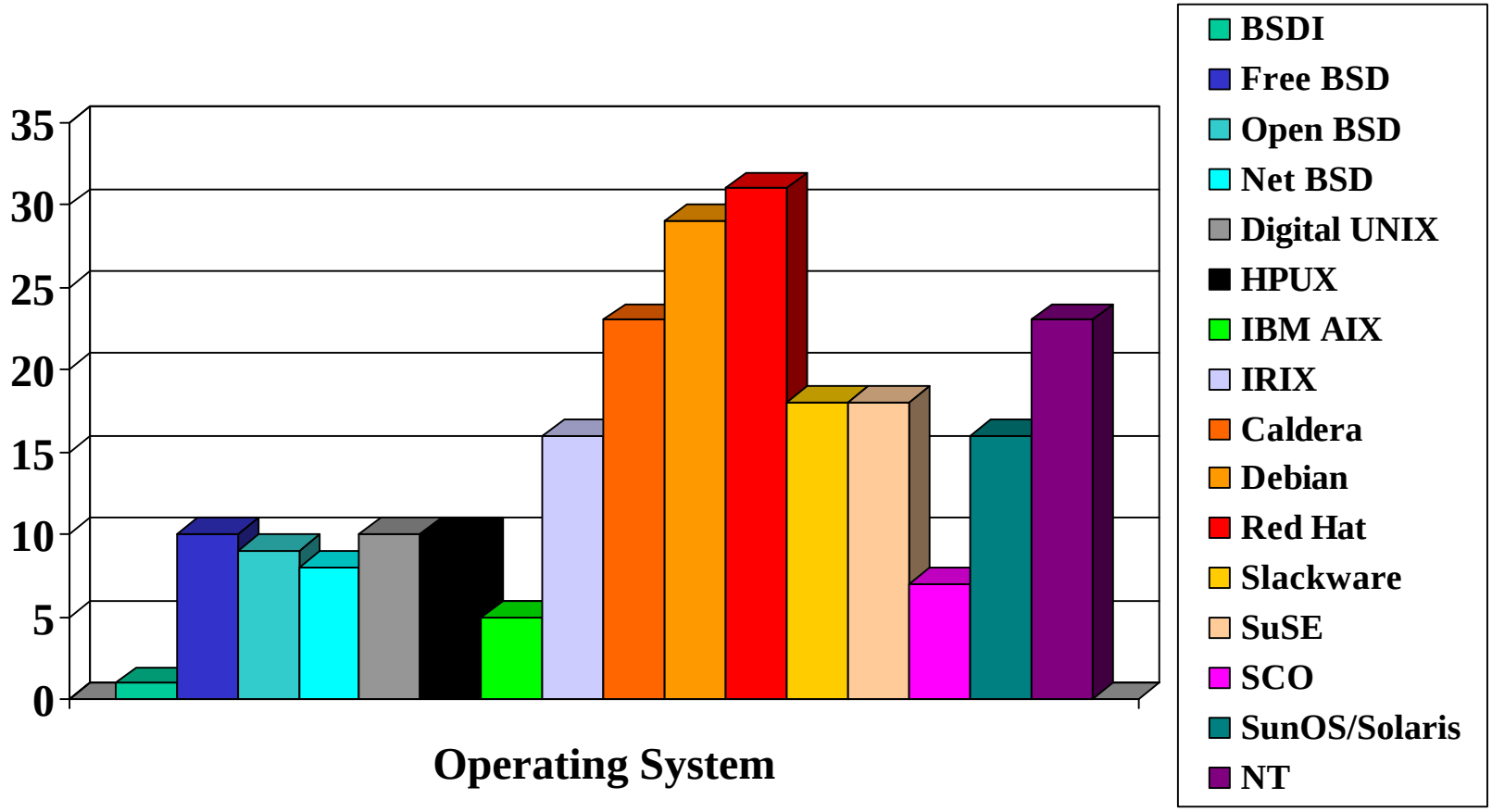


*from Ghosh &O'Connor p 374 NISSC 21

Denial of Service

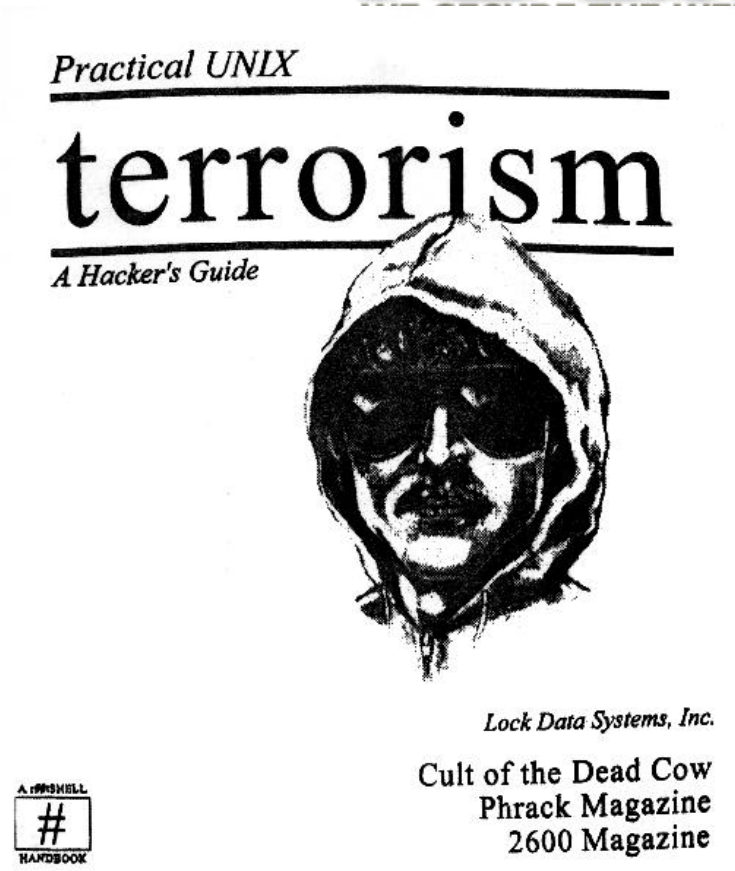
- DDoS
- Network
  - SYN
  - Ping of Death
  - SMURF
  - LAND/BOINK/Teardrop/Newtear/fraggle
  - nuke
- OS & Application

Operating System Vulnerabilities FY 00



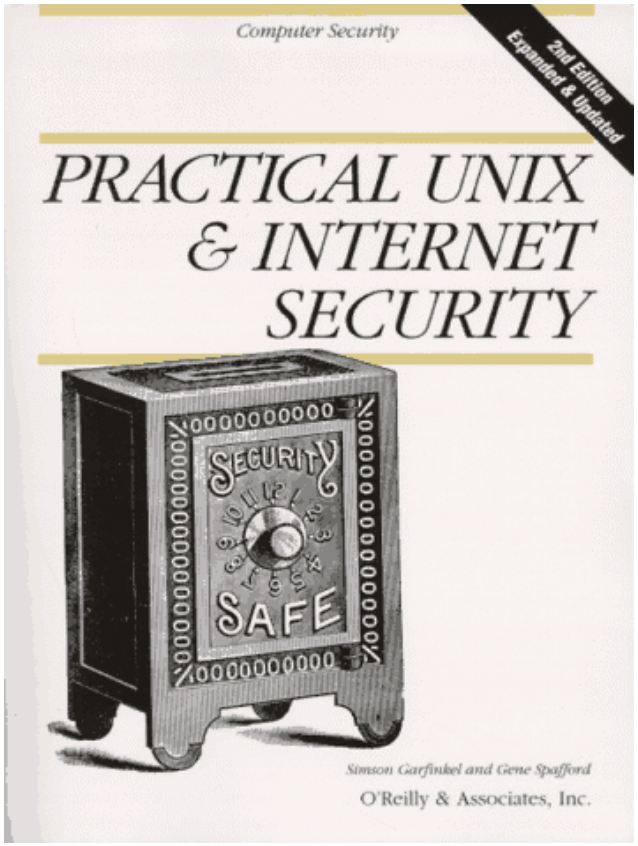
UNIX

- Migration among Distributions
- Reverse engineering
- ftp daemon
- rpc
- Desktops
  - CDE
  - KDE
  - X11



UNIX

- Migration among Distributions
- Reverse engineering
- ftp daemon
- rpc
- Desktops
  - CDE
  - KDE
  - X11



Microsoft Windows NT

- Maturity
- DoS
  - Out of Band
  - Fragments
- Applications
  - IIS
  - FrontPage
  - Cold Fusion
  - IE

Applications

- **BIND**
- **World Wide Web**
  - **Server**
    - **CGI**
    - **Back end processes**
    - **Cold Fusion**
    - **Front Page**
  - **Clients**

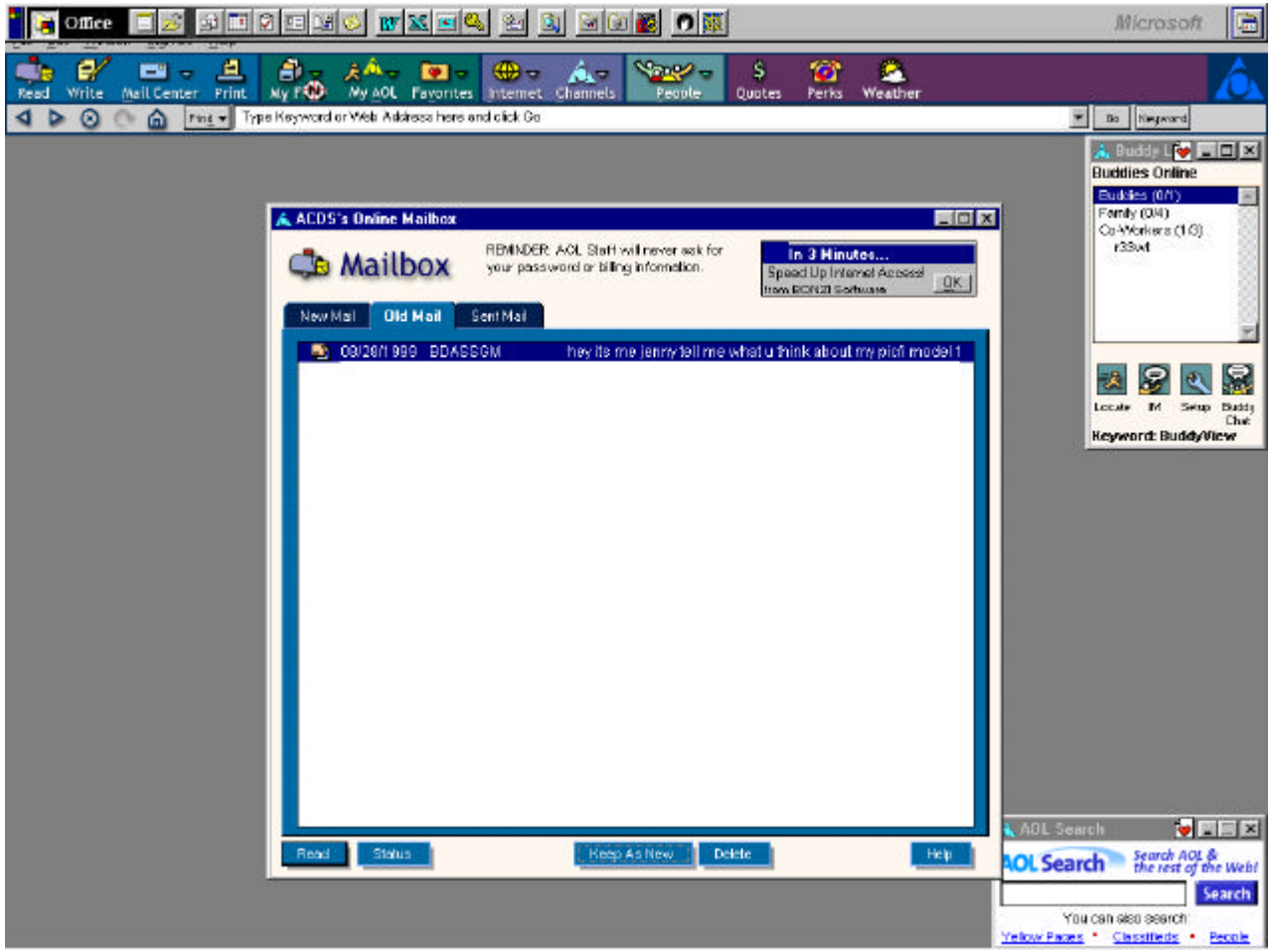
Trojans and Back Doors

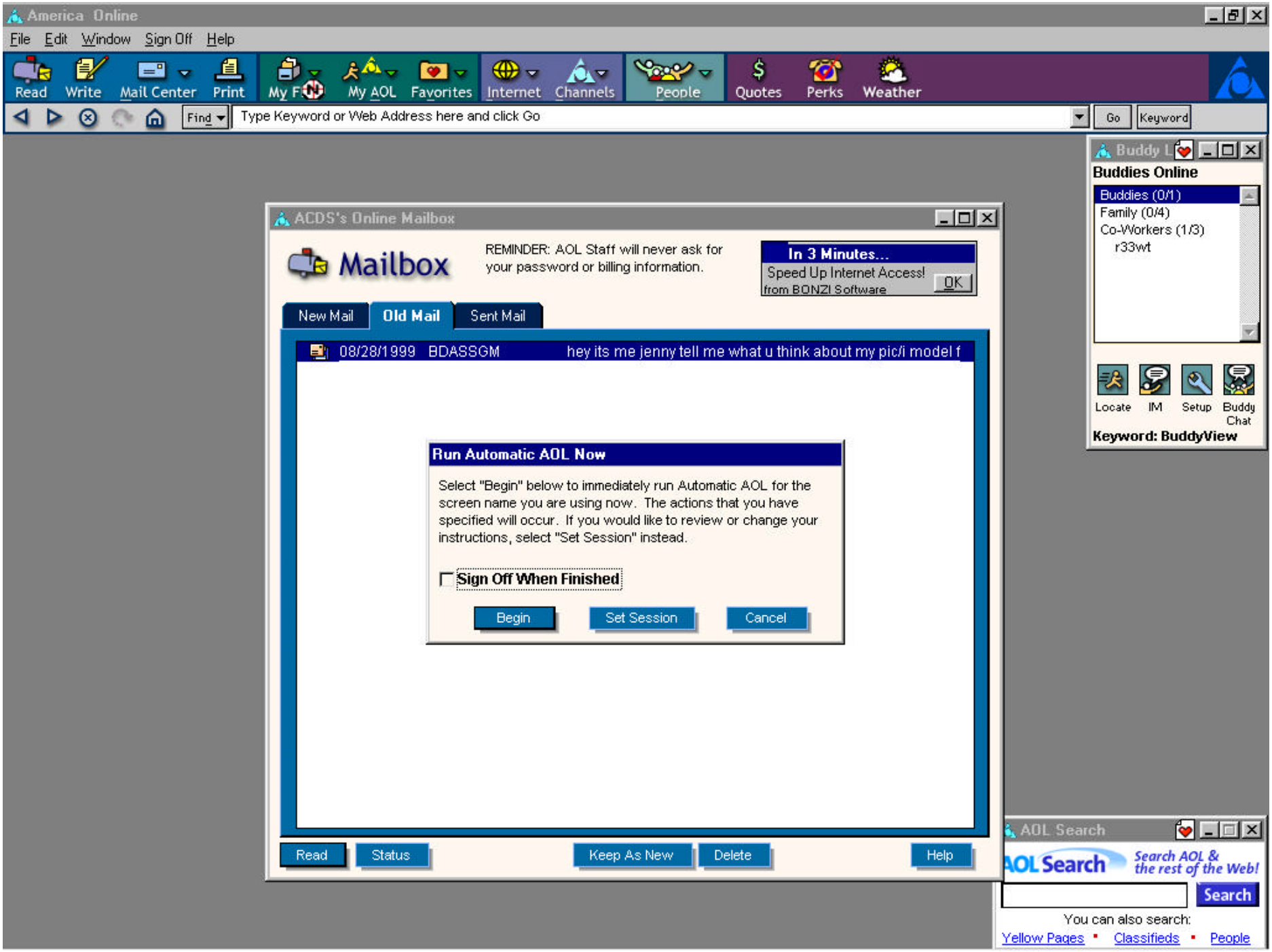
- Backdoor-G
  - most common malcode on USENET
- Back Orifice/BO2
- DIRT ?
- Netbus
- .shs scrap object attachments
- .vbs script objects
- Virus Infections highlight the severity of the vulnerability

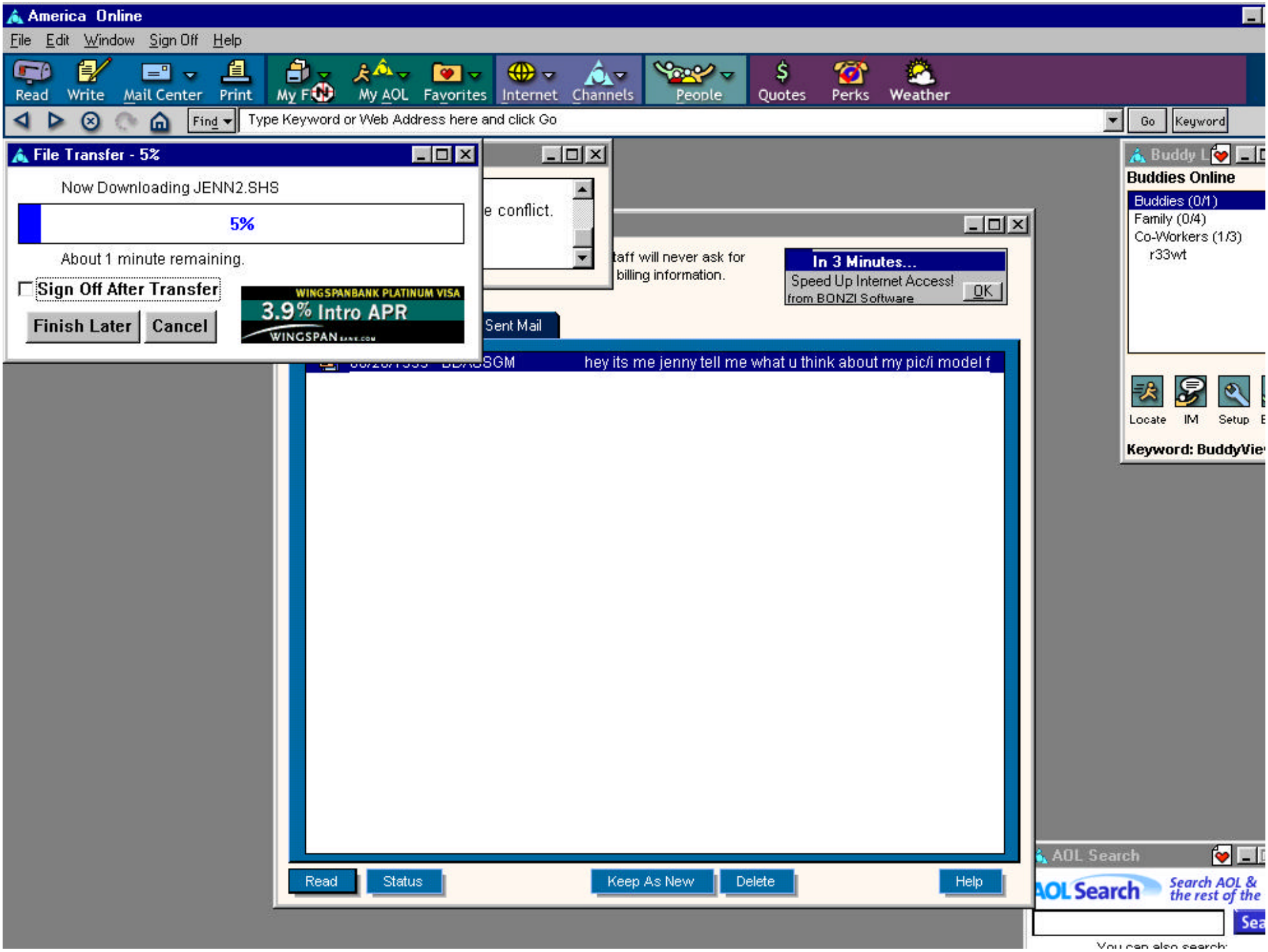
Sir Dystic

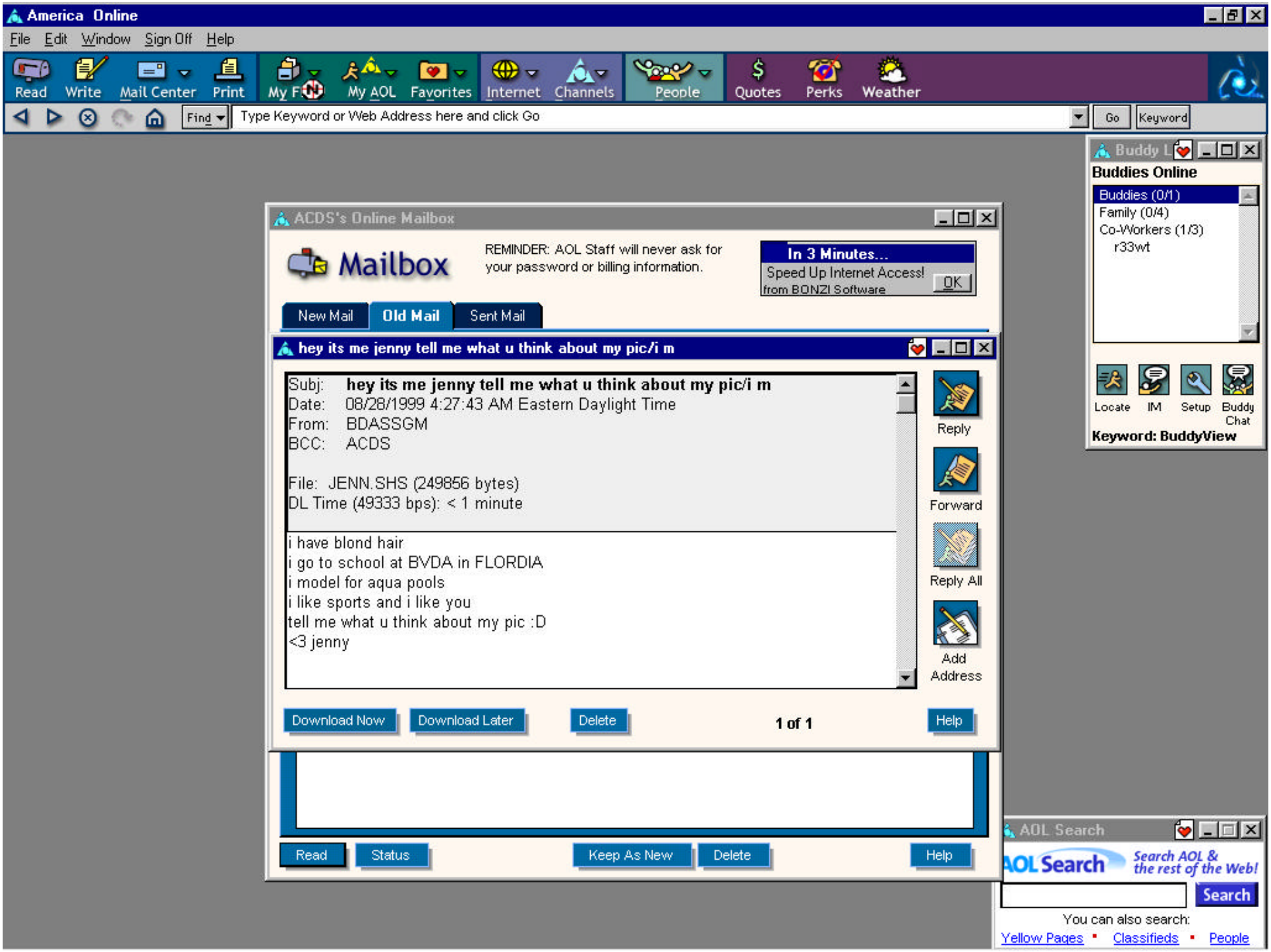
Uh?

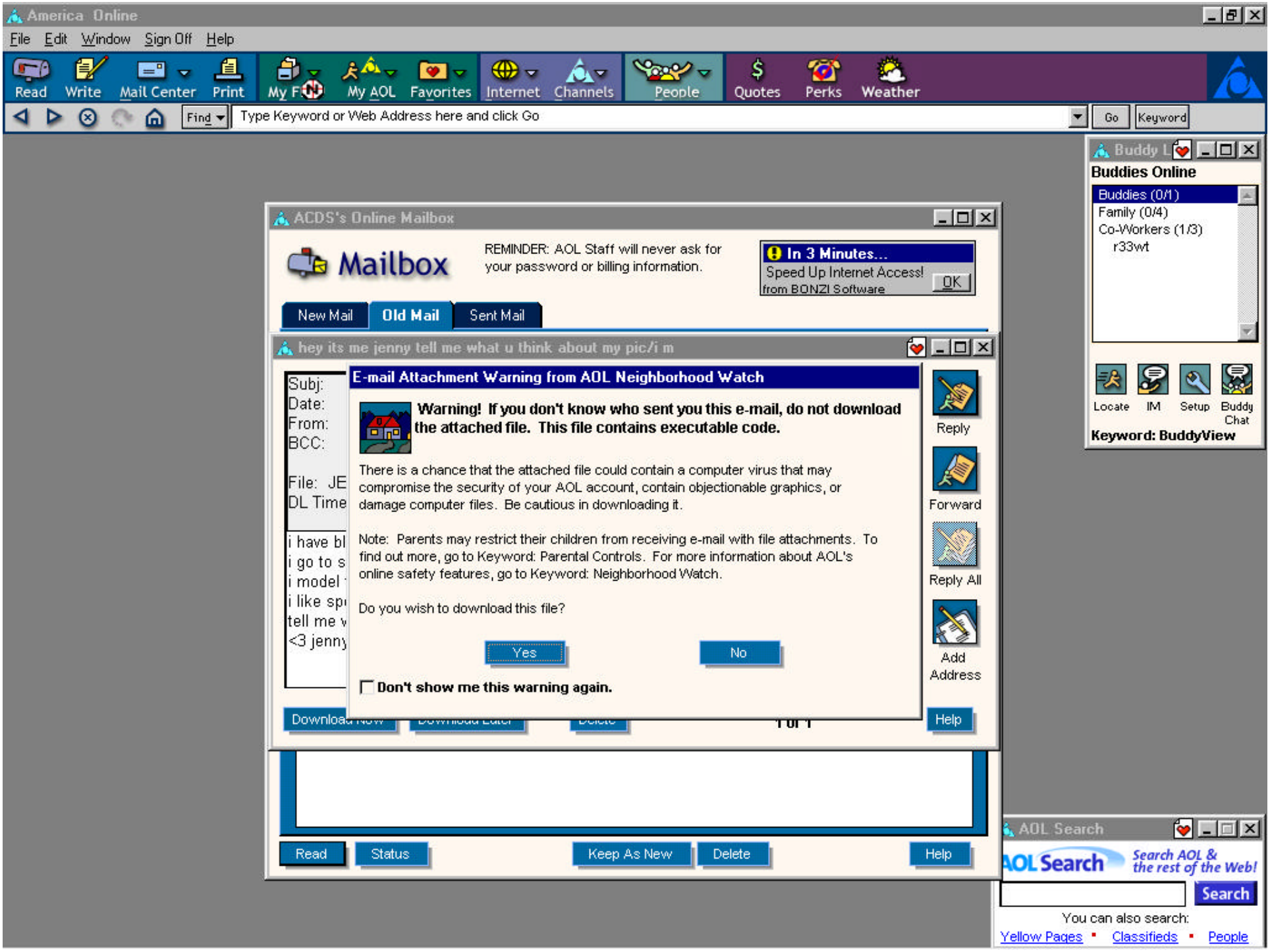
Beware of Geeks...

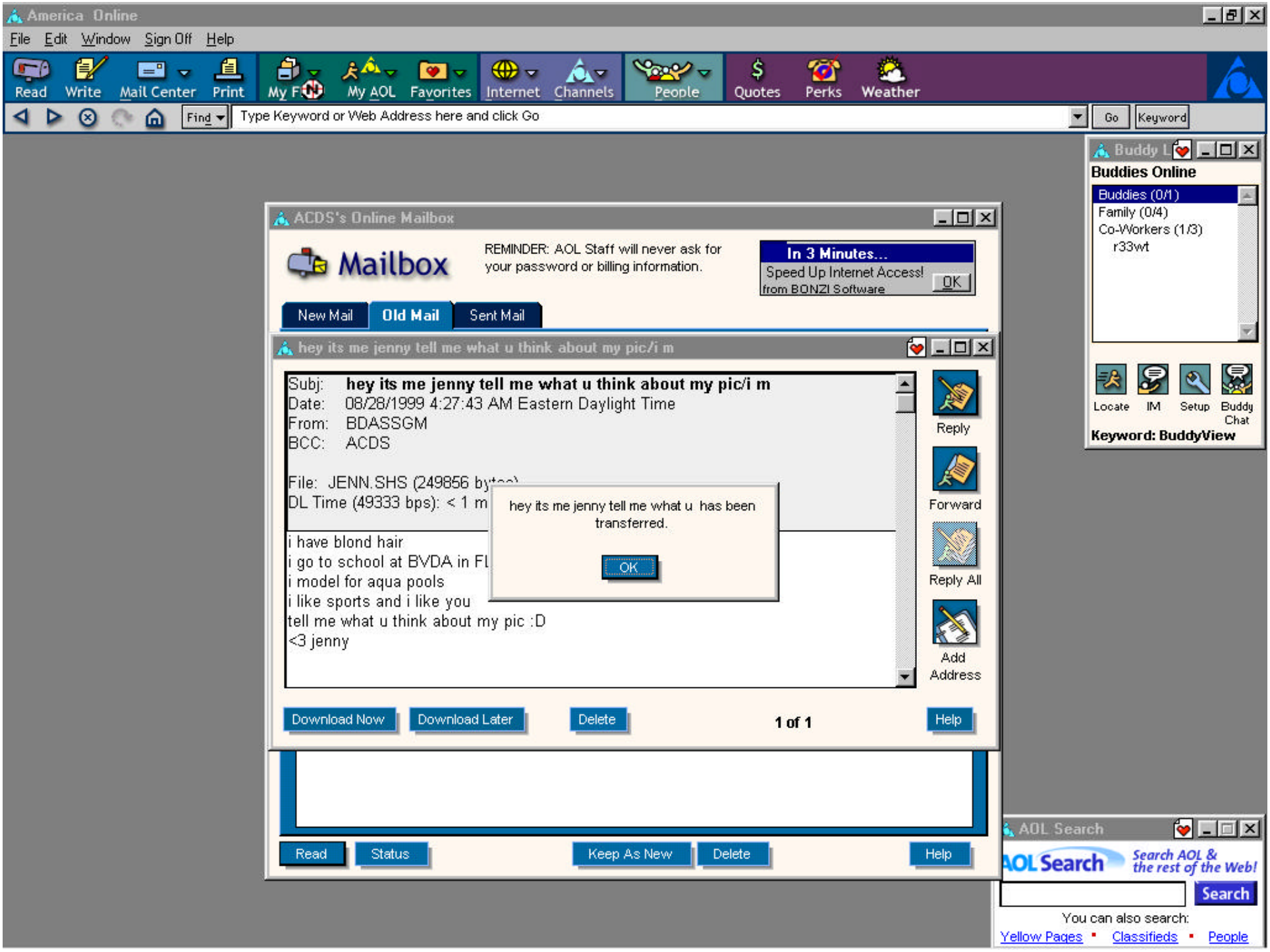



America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My F My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Buddy L
Buddies Online
Buddies (0/1)
Family (0/4)
Co-Workers (1/3)
r33wt
Locate IM Setup Buddy Chat
Keyword: BuddyView
ACDS's Online Mailbox
Mailbox
REMINDER: AOL Staff will never ask for your password or billing information.
In 3 Minutes...
Speed Up Internet Access!
from BONZI Software
OK
New Mail Old Mail Sent Mail
08/28/1999 BDASSGM hey its me jenny tell me what u think about my pic/i model f
Run Automatic AOL Now
Select "Begin" below to immediately run Automatic AOL for the screen name you are using now. The actions that you have specified will occur. If you would like to review or change your instructions, select "Set Session" instead.
Sign Off When Finished
Begin Set Session Cancel
Read Status Keep As New Delete Help
AOL Search
AOL Search
Search AOL & the rest of the Web!
Search
You can also search:
Yellow Pages Classifieds People


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My AOL Favorites Internet Channels People Quotes Perks Weather
Find
Type Keyword or Web Address here and click Go
Go
Keyword
File Transfer - 5%
Now Downloading JENN2.SHS
5%
About 1 minute remaining.
Sign Off After Transfer
Finish Later
Cancel
WINGSPANBANK PLATINUM VISA
3.9% Intro APR
WINGSPAN
e conflict.
taff will never ask for
billing information.
In 3 Minutes...
Speed Up Internet Access!
from BONZI Software
OK
Sent Mail
SGM
hey its me jenny tell me what u think about my pic/i model f
Read
Status
Keep As New
Delete
Help
Buddies Online
Buddies (0/1)
Family (0/4)
Co-Workers (1/3)
r33wt
Locate
IM
Setup
Keyword: BuddyVie
AOL Search
AOL Search
Search AOL &
the rest of the


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My AOL Favorites Internet Channels People Quotes Perks Weather
Find
Type Keyword or Web Address here and click Go
Go
Keyword
Buddy List
Buddies Online
Buddies (0/1)
Family (0/4)
Co-Workers (1/3)
r33wt
Locate IM Setup Buddy Chat
Keyword: BuddyView
ACDS's Online Mailbox
Mailbox
REMINDER: AOL Staff will never ask for your password or billing information.
In 3 Minutes...
Speed Up Internet Access!
from BONZI Software
OK
New Mail
Old Mail
Sent Mail
hey its me jenny tell me what u think about my pic/i m
Subj: hey its me jenny tell me what u think about my pic/i m
Date: 08/28/1999 4:27:43 AM Eastern Daylight Time
From: BDASSGM
BCC: ACDS
File: JENN.SHS (249856 bytes)
DL Time (49333 bps): < 1 minute
i have blond hair
i go to school at BVDA in FLORDIA
i model for aqua pools
i like sports and i like you
tell me what u think about my pic :D
<3 jenny
Reply
Forward
Reply All
Add Address
Download Now
Download Later
Delete
1 of 1
Help
Read
Status
Keep As New
Delete
Help
AOL Search
AOL Search
Search AOL & the rest of the Web!
Search
You can also search:
Yellow Pages
Classifieds
People


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My F My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go Go Keyword
Buddy L
Buddies Online
Buddies (0/1)
Family (0/4)
Co-Workers (1/3)
r33wt
Locate IM Setup Buddy Chat
Keyword: BuddyView
ACDS's Online Mailbox
Mailbox
REMINDER: AOL Staff will never ask for your password or billing information.
In 3 Minutes...
Speed Up Internet Access!
from BONZI Software
OK
New Mail Old Mail Sent Mail
hey its me jenny tell me what u think about my pic/i m
Subj:
Date:
From:
BCC:
File: JE
DL Time
i have bl
i go to s
i model
i like sp
tell me
<3 jenny
E-mail Attachment Warning from AOL Neighborhood Watch
Warning! If you don't know who sent you this e-mail, do not download the attached file. This file contains executable code.
There is a chance that the attached file could contain a computer virus that may compromise the security of your AOL account, contain objectionable graphics, or damage computer files. Be cautious in downloading it.
Note: Parents may restrict their children from receiving e-mail with file attachments. To find out more, go to Keyword: Parental Controls. For more information about AOL's online safety features, go to Keyword: Neighborhood Watch.
Do you wish to download this file?
Yes
No
Don't show me this warning again.
Reply
Forward
Reply All
Add Address
Help
1 of 1
Read Status Keep As New Delete Help
AOL Search
AOL Search
Search AOL & the rest of the Web!
Search
You can also search:
Yellow Pages Classifieds People


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My F My AOL Favorites Internet Channels People Quotes Perks Weather
Find Type Keyword or Web Address here and click Go
Go Keyword
Buddy L
Buddies Online
Buddies (0/1)
Family (0/4)
Co-Workers (1/3)
r33wt
Locate IM Setup Buddy Chat
Keyword: BuddyView
ACDS's Online Mailbox
Mailbox
REMINDER: AOL Staff will never ask for your password or billing information.
In 3 Minutes...
Speed Up Internet Access!
from BONZI Software
OK
New Mail Old Mail Sent Mail
hey its me jenny tell me what u think about my pic/i m
Subj: hey its me jenny tell me what u think about my pic/i m
Date: 08/28/1999 4:27:43 AM Eastern Daylight Time
From: BDASSGM
BCC: ACDS
File: JENN.SHS (249856 by
DL Time (49333 bps): < 1 m
hey its me jenny tell me what u has been transferred.
OK
i have blond hair
i go to school at BVDA in Fl
i model for aqua pools
i like sports and i like you
tell me what u think about my pic :D
<3 jenny
Reply
Forward
Reply All
Add Address
Download Now Download Later Delete 1 of 1 Help
Read Status Keep As New Delete Help
AOL Search
AOL Search
Search AOL & the rest of the Web!
Search
You can also search:
Yellow Pages Classifieds People

Bering Gifts

Nightmares

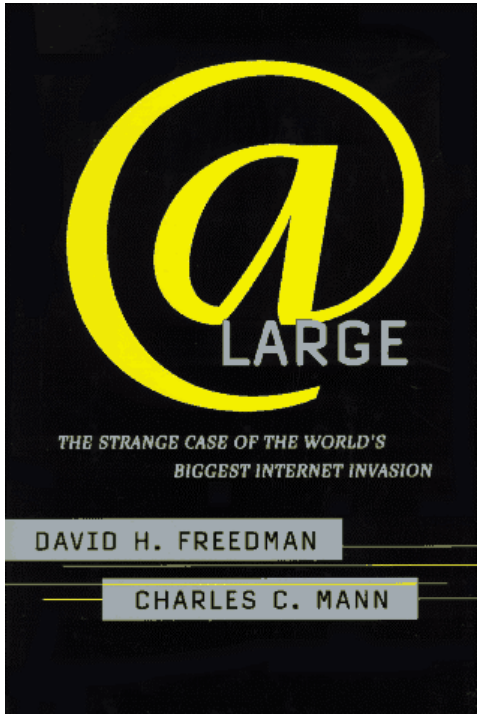
- Sophisticated scans
- Evil genius
- Collaboration
- Mentor
- Oh Gooey-gooey!

Basics

- Passwords (The road to damnation is paved with good intentions)
- Gratuitous functions
- Hardware has never been cheaper
- Currency (it's more than money)
- Better is the Enemy of Good
- Salaries count
- Risk Management not Risk Avoidance!

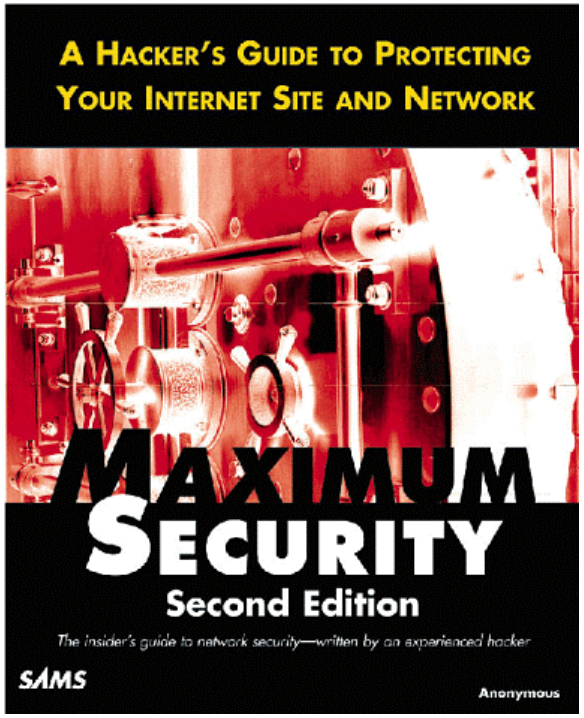
Suggested Reading

At Large



$10.40

Maximum Security



$39.99

Contact

dkennedy@icsa.net

PGP Key ID:**0x2C72226D**

PGP Fingerprint:

45FB CB2C 37C9 D2AF 1FE6 C089 A490 2F82