

# VT INFOSAFE



Champlain College  
Norwich University

Federal Bureau of Investigation  
Vermont Army National Guard

Vermont Information Technology Center

The screenshot shows a Windows desktop with a blue sky and ocean background. On the left is a taskbar with icons for My Documents, My Computer, My Network Places, Recycle Bin, Adobe Acrobat 5.0, AOL Instant Messenger, Burn CDs & DVDs with..., hp officejet series, Logitech QuickCam, and Unused Desktop. The main window is titled "Quicken Deluxe 98 - HAS - [Checking - Hanley Allen Strappman: Bank]". The window displays a table of transactions for a checking account.

Date	Num	Payee / Category / Memo	Payment	Clr	Deposit	Balance
05/01/04	DEP	W/Depos, Etc.			3,315.22	4,430.69
		--Split--				
05/01/04	457	American Express #1234-567890-54321	123.98			4,306.91
		--Split--				
05/01/04	458	1st Bank Of Colchester Mortgage #R04-156720	550.00			3,756.91
05/01/04	459	VISA Household #6574-8332-0129-3847	65.32			3,691.59
05/01/04	460	Colchester Junior High School Education Hanley Jr. field trip	10.00			3,681.59
05/01/04	461	Fletcher Allen Health Care Medical Doctor 1/29 surgery (#2)	45.67			3,635.92
05/03/04	462	Guns & Ammo Subscriptions	12.29			3,623.63
05/03/04	463	GCK Travel Vacation down payment	400.00			

The window also shows a toolbar with buttons for Delete, Find, Transfer, Reconcile, Edit Account, Report, and View. At the bottom of the window, there are buttons for Accounts, Bills, Planning, Investments, Home & Car, Online, and Reports. The ending balance is shown as 3,623.63.

## Evolution of Home Networks

- Multiple computers in the home on the rise
  - Many ways to network systems together
  - Windows and MacOS expedite file sharing
- Concurrent growth in business and personal use of the Internet from home
- **Security issues are on the rise!!**

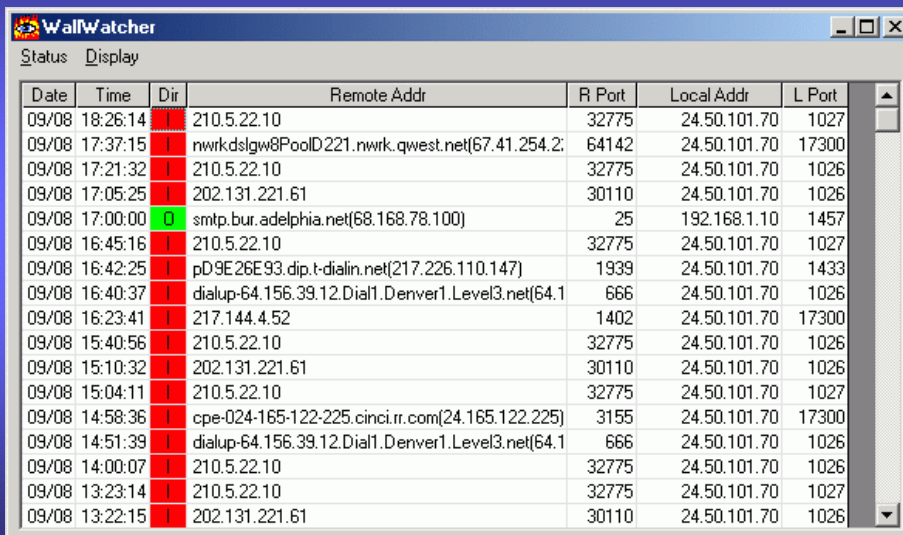
## "Always On" Network Connections

- As availability increases and prices drop, more and more homes are being wired for ADSL and cable modems
- *Always on* network connections make your home computer/network *always exposed*
  - Most users do not realize their exposure
  - Most ISPs do not educate their users

# What's At Risk?

- What might be found on your computer?
  - Private communications
  - Medical records
  - Financial records
  - Family information
- The risks?
  - Identity theft/fraud
  - Your computer as storage
  - Your computer used to attack others

# A Day in the Life...At Home



The screenshot shows the WallWatcher application window with a table of network connection logs. The table has columns for Date, Time, Dir, Remote Addr, R Port, Local Addr, and L Port. The data shows various incoming connections from different IP addresses and ports, with most being blocked (indicated by a red 'I' icon) and one being allowed (indicated by a green 'D' icon).

Date	Time	Dir	Remote Addr	R Port	Local Addr	L Port
09/08	18:26:14	I	210.5.22.10	32775	24.50.101.70	1027
09/08	17:37:15	I	nwrkdsigw8PoolD221.nwrk.qwest.net(67.41.254.2)	64142	24.50.101.70	17300
09/08	17:21:32	I	210.5.22.10	32775	24.50.101.70	1026
09/08	17:05:25	I	202.131.221.61	30110	24.50.101.70	1026
09/08	17:00:00	D	smtp.bur.adelphia.net(68.168.78.100)	25	192.168.1.10	1457
09/08	16:45:16	I	210.5.22.10	32775	24.50.101.70	1027
09/08	16:42:25	I	pD9E26E93.dip.t-dialin.net(217.226.110.147)	1939	24.50.101.70	1433
09/08	16:40:37	I	dialup-64.156.39.12.Dial1.Denver1.Level3.net(64.1	666	24.50.101.70	1026
09/08	16:23:41	I	217.144.4.52	1402	24.50.101.70	17300
09/08	15:40:56	I	210.5.22.10	32775	24.50.101.70	1026
09/08	15:10:32	I	202.131.221.61	30110	24.50.101.70	1026
09/08	15:04:11	I	210.5.22.10	32775	24.50.101.70	1027
09/08	14:58:36	I	cpe-024-165-122-225.cinci.rr.com(24.165.122.225)	3155	24.50.101.70	17300
09/08	14:51:39	I	dialup-64.156.39.12.Dial1.Denver1.Level3.net(64.1	666	24.50.101.70	1026
09/08	14:00:07	I	210.5.22.10	32775	24.50.101.70	1026
09/08	13:23:14	I	210.5.22.10	32775	24.50.101.70	1027
09/08	13:22:15	I	202.131.221.61	30110	24.50.101.70	1026

## Home users affect Critical Infrastructure

- May 5th, 2004
  - 24 hours of Sasser
  - 70,296 attack attempts
  - 15,582 different attackers
  - 99.8% from DSL/Cable/Dial users
  - Affected flights, shipping, and banking systems
- Unprotected life expectancy < 10 minutes

## What Are We Concerned About?

- Viruses
- Trojans
- Worms
- Spyware
- Wireless networking
- Kids' privacy and safety
- Scams, e-fraud

# Some Personal System Guidelines

The situation is *not* hopeless!!!!

1. Employ anti-virus software
2. Employ personal firewall software or hardware
3. Keep your operating system patches up-to-date
4. Employ spyware-detection software
5. Educate your family and develop safe-networking practices
6. Never give out personal information over the Internet unless you are very sure to whom you are giving it
7. Never open an e-mail attachment unless it comes from someone you know **and** you are expecting it
8. Make backups of your critical data

## VT INFOSAFE

- **VT INFOSAFE** is the Vermont InfraGard chapter's effort to education home users about the
  - Importance of information security
  - Potential pitfalls of using the Internet
  - Ways to protect oneself on the Internet
- Why do this?
  - Residential information security has implications for homeland security, law enforcement, and infrastructure protection
  - We wouldn't let people drive a car without a driver's license....
- The first state-wide initiative of its kind