Cyber Security
For Lawyers and Law Offices

Russell Jackman, Esq.

Your Presenter: Russell Jackman, Esq.

- **Consultant:** Law offices and Attorneys throughout California
- **Lecturer:**, State Bar of CA, LACBA, CA Paralegals Association, numerous MCLE providers.
- **Head Technology Trainer:** Weil, Gotshal & Manges
- **Vice Chair:** Law Practice Management & Technology Section- State Bar of CA
- **Professor:** Cal State Hayward, College of Marin, St. Mary's University-Moraga, SF State University

ABA RULES

ABA Model Rule 1.1 Competence: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

ABA Model Rule 1.6(c), "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

2.http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

Computer Security in the Law office: Why?

- Why Should I be concerned with Computer Security at all?

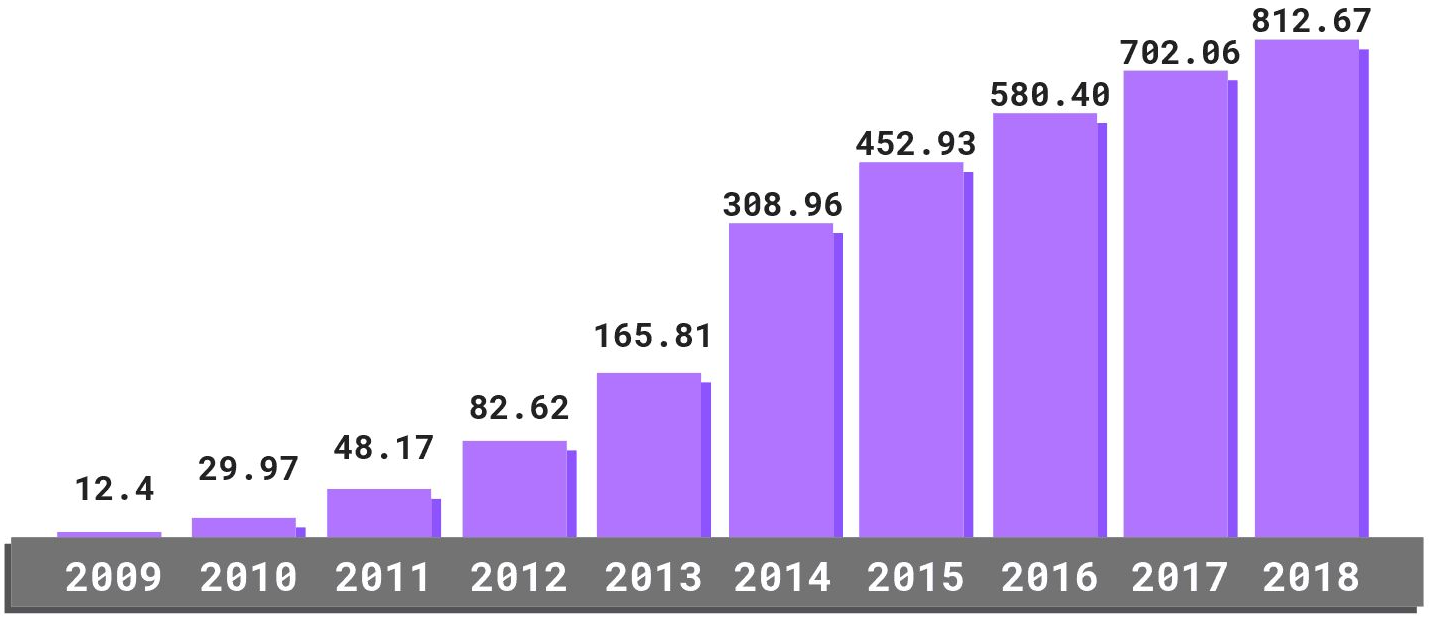
In 1999, the "Melissa" virus hijacked victims' e-mail address books to replicate itself, infecting 1 million PCs overnight and causing $80 million in damage.

Computer Security in the Law office: Why?

In 2000, the "I Love You" virus didn't just mail itself to users' business customers, colleagues, friends and family; *it also mailed passwords* to the virus' creator.

"I Love You" hit every business sector, from Fortune 100 companies to the Department of Defense, causing an estimated **$8.75 billion** in damage.

Philip Ross:*Businesses can ill afford computer virus;* **Chicago Sun-Times** *March 15, 2005*



Total Malware Infection Growth Rate (In Millions)

Malware attacks shoot up

by Phil Muncaster

16 Apr 2009

Be the first to comment

Last year saw another staggering rise in malicious software, with more than 1.6 million new threats created, according to the latest *Internet Security Threat Report* from Symantec.

The security specialist's 2008 study found malware grew more than 200 per cent from 2007, while botnet activity rose by 47 per cent.

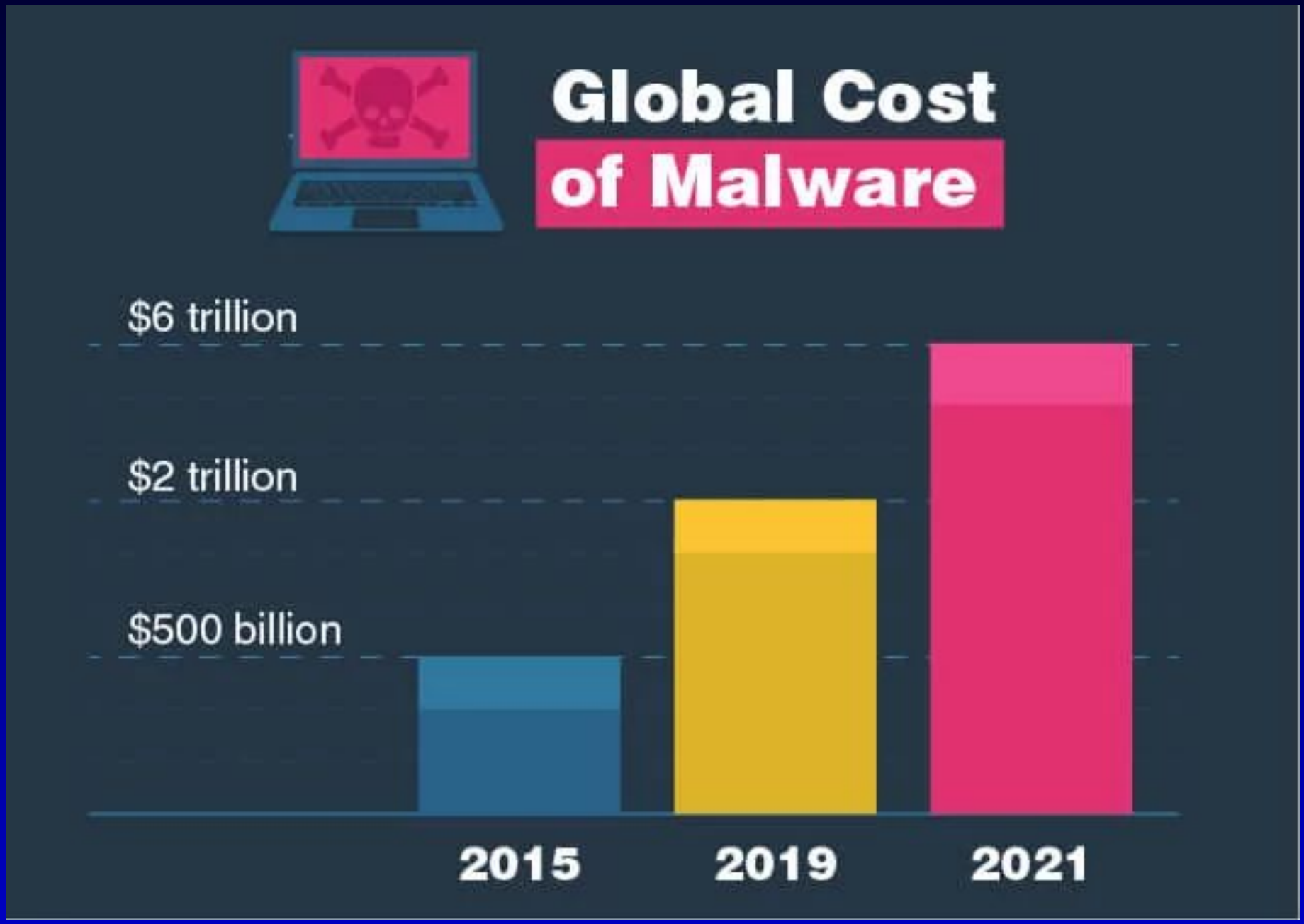
Cyber Crime Costs $114B Per Year, Mobile Attacks on the Rise

BY CHLOE ALBANESIUS SEPTEMBER 7, 2011 03:02PM EST 2 COMMENTS

How much do cyber attacks actually cost? According to a new study from Symantec, it's a whopping $114 billion each year.

With reports of Anonymous and LulzSec data dumps and digital certificate hacks in the headlines, it should be no surprise that cyber crime is a real threat. But how much do these Web attacks actually cost? According to a new study from Symantec, it's $114 billion each year.

If you count time lost by companies trying to recover from cyber attacks, meanwhile, you can add another $274 billion to that number.


Global Cost
of Malware
$6 trillion
$2 trillion
$500 billion
2015
2019
2021

But the threats are being ignored

WASHINGTON and MOUNTAIN VIEW, Calif. - October 15, 2012 - U.S. small business owners or operators have a false sense of cybersecurity as more than three-fourths (77 percent) say their company is safe from cyber threats such as hackers, viruses, malware or a cybersecurity breach, **yet 83 percent have no formal cybersecurity plan**. These findings are from a new survey released today of 1,015 U.S. small- and medium-sized businesses (SMBs) by the National Cyber Security Alliance (NCSA) and Symantec.

- **A Majority of SMBs Believe Security Is Critical to Their Success and Brand:** Seventy-three percent of SMBs say a safe and trusted Internet is critical to their success, and 77 percent say a strong cybersecurity and online safety posture is good for their company's brand.
- **SMBs Unprepared to Handle Data Breach Losses:** Nearly six out of 10 (59 percent) SMBs do not have a contingency plan outlining procedures for responding and reporting data breach losses.
- **Two-thirds of SMBs Aren't Concerned About Cyber Threats:** Sixty-six percent of SMBs are not concerned about cyber threats – either external or internal. External threats include a hacker or cyber-criminal stealing data while internal threats include an employee, ex-employee, or contractor/consultant stealing data.

http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

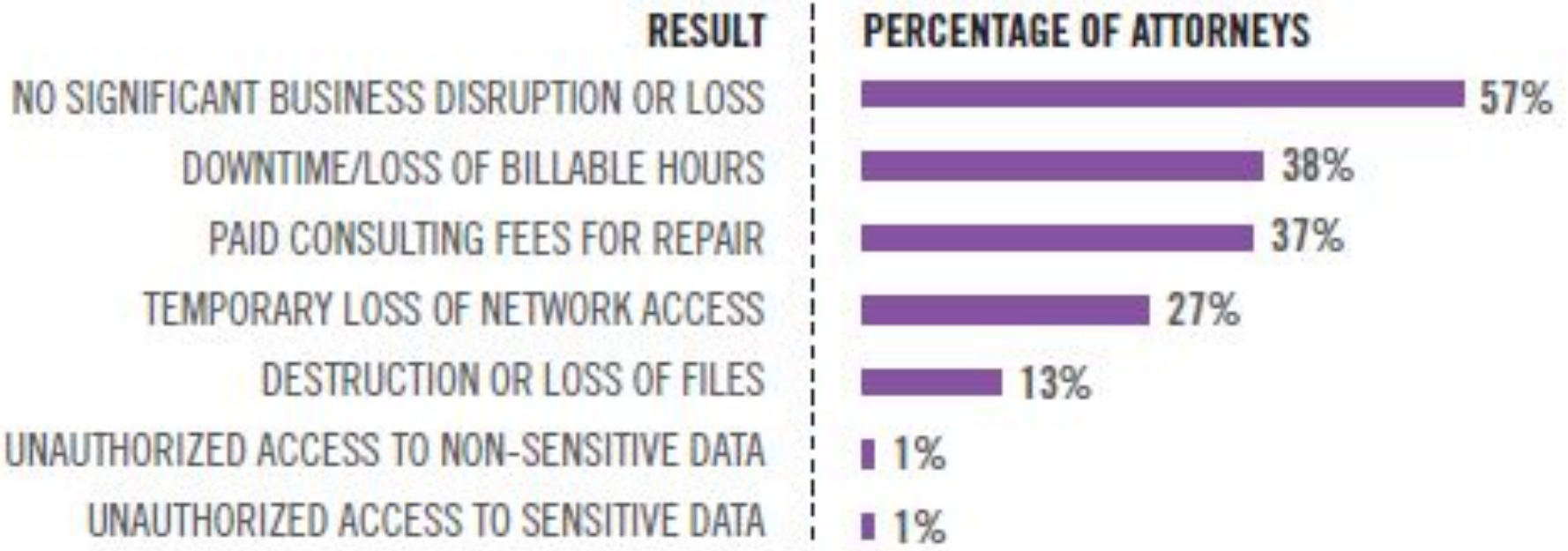
The 2017 Survey also inquired about viruses/spyware/malware infections.

Overall, 43% reported infections, 34% reported none, and 23% reported that they don't know.

Reported infections were greatest in firms with 10-49 attorneys (63%), 2-9 (53%), and approximately 30% in other firms. Infections can cause serious consequences, including compromise of confidentiality and loss of data.

Source: American Bar Association
https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/

IF YOU HAVE BEEN HIT BY MALWARE, WHAT WAS THE RESULT?



Still, it's not MY computer here at the office

Or is it…?

Do you…?

Use the same ID/password at the office that you use at home?

check your private email at the office?

save one-of-a kind files on your work computer?

have better things to do than to deal with lost hours, research and work?


WORKING DAZE
JOHN ZAKOUR
SCOTT ROBERTS
OMIGOSH! THERE'S A PROBLEM WITH MY BANK ACCOUNT! I NEED TO GO TO THIS PAGE AND TYPE IN ALL MY...
HEY!
SMACK
THANK YOU, DANA. I KEEP FORGETTING.
THE COMPANY ONLY JUST GOT BACK ONLINE SINCE THE LAST VIRUS YOU OPENED AND YOU JUMP RIGHT IN THE NET.
ZAKOUR ROBERTS 10-18

If so, YOU could be at risk

- Viruses don't care who they effect
- Hackers can take any info that comes through your computer and use it for their own purposes
- Spyware & Adware clog up your system and make it difficult to research
- Lockups/Restarts/**Lost Data**

"But all I ever use is my instant messenger…"

"Users of instant messaging software must run up-to-date virus protection software on their desktop computers, as well as exercising caution about what they choose to run or click on."

Graham Cluley, senior technology consultant for Sophos

Same Story, Different Year…

Mailboxes in Germany and the Netherlands were flooded yesterday with spam containing German right-wing propaganda. Spammers used the Sober.G virus - a mass mailing worm that sends itself to email addresses harvested from infected computers - to spread their messages as widely as possible.

Analysts think the spammers may have worked in tandem with virus programmers to ***hijack PCs and use addresses found there to build large distribution lists. This is believed to be the first time that right wing extremists have used spamming systematically to reach a broad audience***. The sheer size of the operation stunned many experts.

By *Jan Libbenga*, The Register Jun 11 2004 8:27AM

AND AGAIN IN 2005!

Virus writers turned PCs infected with the Sober-P worm into relay stations for right-wing propaganda using backdoor access into compromised machines to load malicious code.

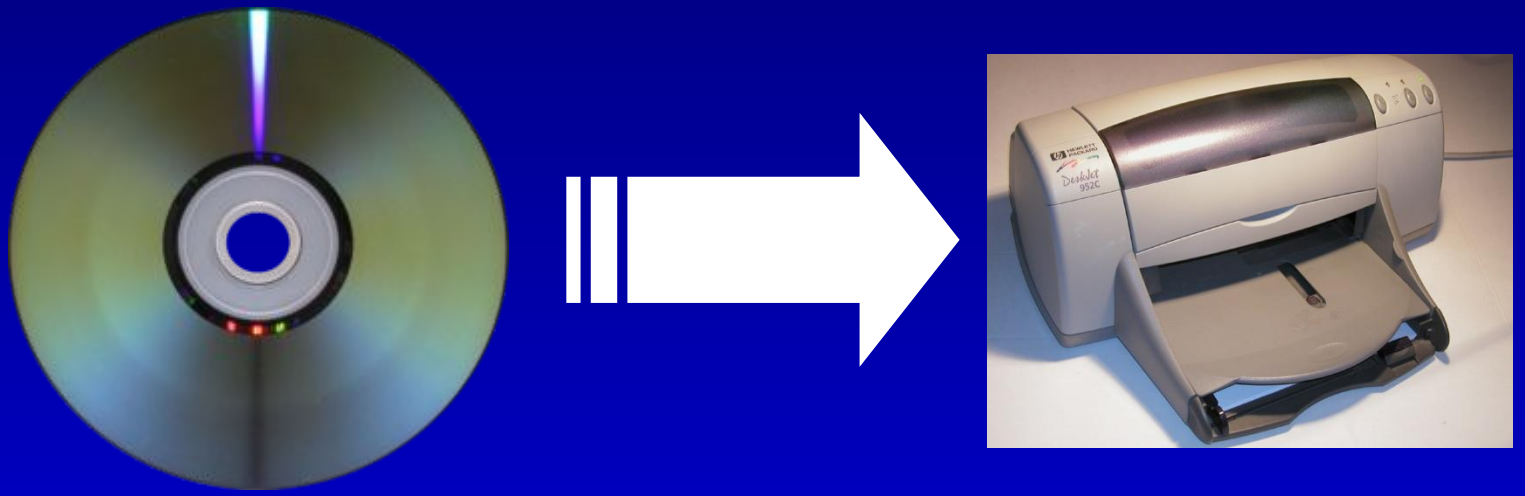
Sober-Q was downloaded from Saturday (14 May) onwards onto computers infected by recent Sober-P worm. The mass mailing Sober-P worm ***tricked recipients into thinking they had won tickets to the 2006 World Cup football tournament***, duping numerous victims since its first appearance on 2 May.

John Leyden, The Register May 16 2005 7:27AM

Computer virus costs Filipino lawyer his case

In a resolution last month, the Supreme Court upheld an earlier Court of Appeals ruling denying a litigant's pleading for a deadline extension for filing a petition after a computer virus deleted it, according to the High Court's website…"The petitioner's lawyer", said the High Court, "would not have encountered a problem if he had ***been systematic in his work****, as he could have saved the encoded petition in a diskette and printed it."*

By Erwin Lemuel Oliva (Mar 04, 2005)



http://www.pctools.com/spyware-doctor-enterprise/calculate/

Current number of users (computers) in the network:	
Estimated number of instances of Spyware infection in a month	
Estimated time (in hours) per month dedicated to removal of each spyware incident:	
Estimated number of computer crashes in a month:	
Estimated time (in hours) required to restore a computer after a crash:	
Estimated average cost of 1 hour of remediation time:	$
Estimated time (in hours) on support calls due to spyware and malicious infections in a month:	
Estimated cost for 1 hour of support call services:	$
Estimated downtime each month (in hours) of an employee experiencing spyware problems:	
Estimated average cost for 1 hour of employee downtime:	$

Total Annual Cost of Spyware:

Total Annual Cost Per User:

Calculate

Who is doing this?

- Hackers
  - That's where the $ is
  - With so much financial information on the internet, it's easier to steal a bank's worth of information with a computer than with a gun

John Dillinger
Legendary Bank Robber

Who is doing this cont.

- Disgruntled employees
  - They have access, passwords and a reason to cause problems
  - sometimes to cover their own tracks/misdeeds
  - to get "revenge" for being treated poorly

Who is doing this cont.

- Teens/Curious/Braggarts
  - Obtaining social status by creating havoc or problems that get on the news
  - Trying to see if they can duplicate what they've read/heard about
  - Appetite for destruction!

"I love you" virus author

Melissa virus author

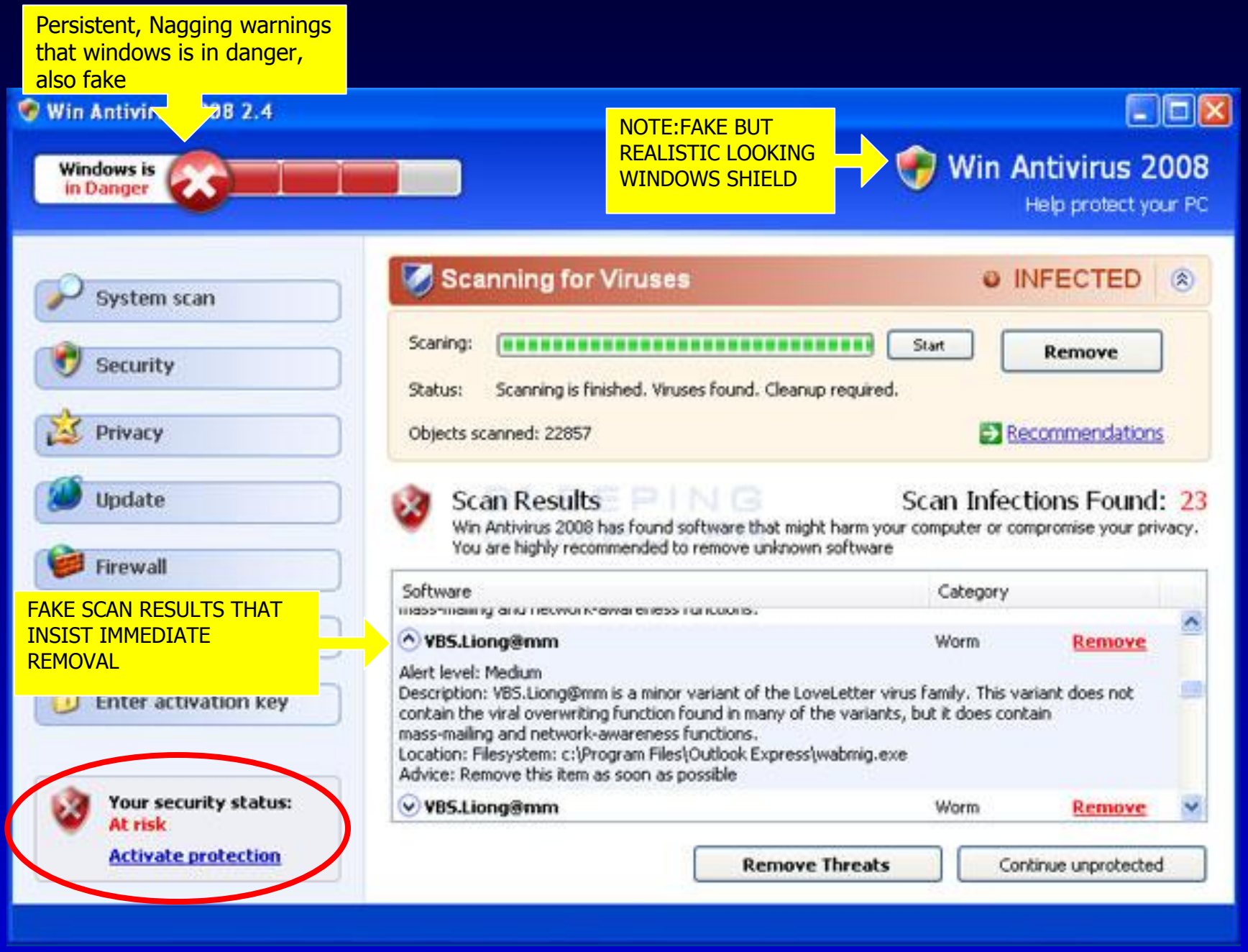
Who is doing this cont.

- Suckers born every minute
  - Spammers work on percentages
  - If they send out 1,000,000 spam messages but only get 1/10th of a % response, that is still 1,000 responses
  - Spam lists of email addresses easily obtained (both legally and illegally)
    - If 1,000 people respond and send $10, spammer gets $10,000
    - Cost for spam software $25-$100

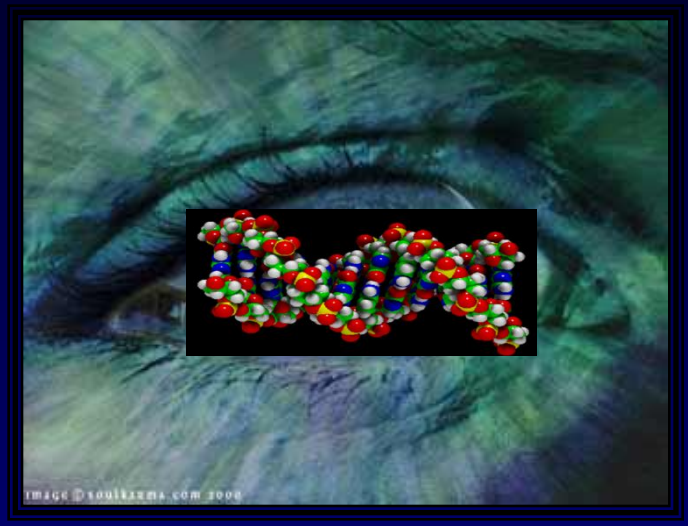
What do they want?

- Your information
- Take over your computer
  - Virtual Joy-Ride using your system as the free vehicle
  - When the police trace it back to your IP address, you are the one forced to explain
- Slow your computer down or stop it entirely
  - many cases people are suckered into buying cheap rip-off programs to stop the virus attack (adware continuously bugging you that your computer is infected, even if McAfee/Norton says otherwise)

EXAMPLE OF RANSOMWARE



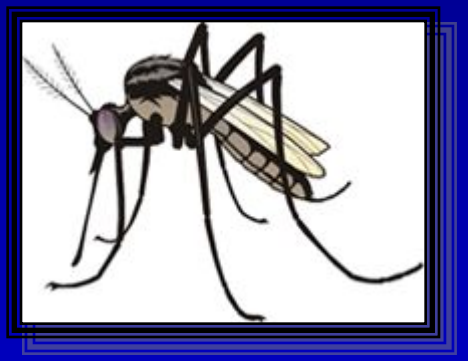
What are Viruses?



- Malware=Any bad software on your computer
- Created by someone outside of your computer
- Purposes=spy on your computer, take information, hijack computer (*BOTNETS*) or crash it

Viruses come in many types

- According to McAfee, over 100,000 different types of threats exist today
- Understanding what threats exist can help protect against infections
- Bad habits and misinformation spread viruses and spyware.



WORMS



- A generic term used to define self-replicating programs
- "mydoom" was a famous one (January 2004)
  - It found the email address book in outlook and mailed a copy of itself to everyone on the list
    - "*The attachment came from someone I trusted*"

BUGS/Exploits

- They exploit flaws in the software or hardware in your computer
- They make the computer crash, can erase hard drives or make it run very *SLOWLY*
- are usually fixed by applying PATCHES supplied by the makers of the exploited software/hardware systems

hijackers

- Take over your “home page” to force it open up to other websites
- Sometimes poor search engines, sometimes porn or download pages
- can disable your internet explorer by forcing you to go only to preset pages or repeatedly reopening explorer again and again.

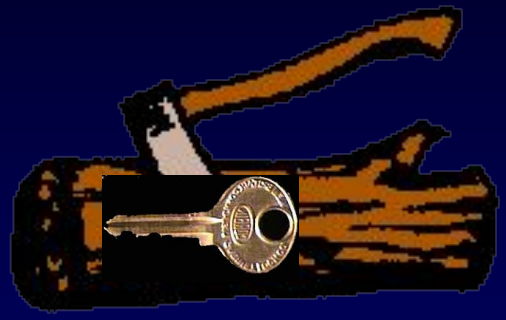
AdWare

- Brings ads and other garbage to your system
- Slows down your internet access
- Creates holes that can be exploited by hackers and other malware
- Beware of someone offering free software or jokes with attachments

TROJAN HORSES & BACKDOORS

- These files break down security
- They open up the different levels of protection
- They allow hackers to gain access to files, data, passwords

Trojan Behavior



- Many times user will not see any performance changes
- Trojans can invite viruses to come in and infect
- “Key Loggers”- keep track of EVERY key stroke for days and then sends an email to a hacker to recreate all your steps!

How can I protect myself?

- Avoid downloading programs from the internet
- Avoid web pages with heavy pop ups and requests for downloads
- Try not to have others bring software from home without authorization
- Keep an eye out for anything that is out of the ordinary

What is Antivirus Software?

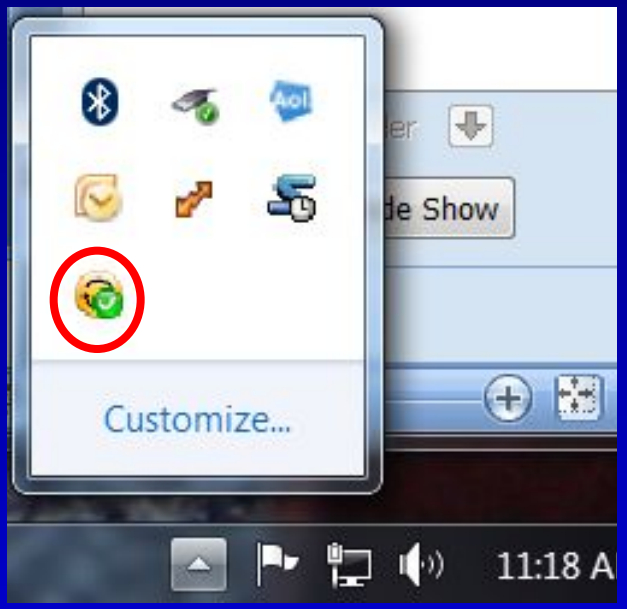
- It acts like a burglar alarm
- Identifies virus (names it)
- Stops Virus from infecting further files
- Gives user options to clean, delete or quarantine file
- Examples: Norton (symantec), McAfee, Panda, Sophos, AVG, Windows Security Essentials

How does it work?

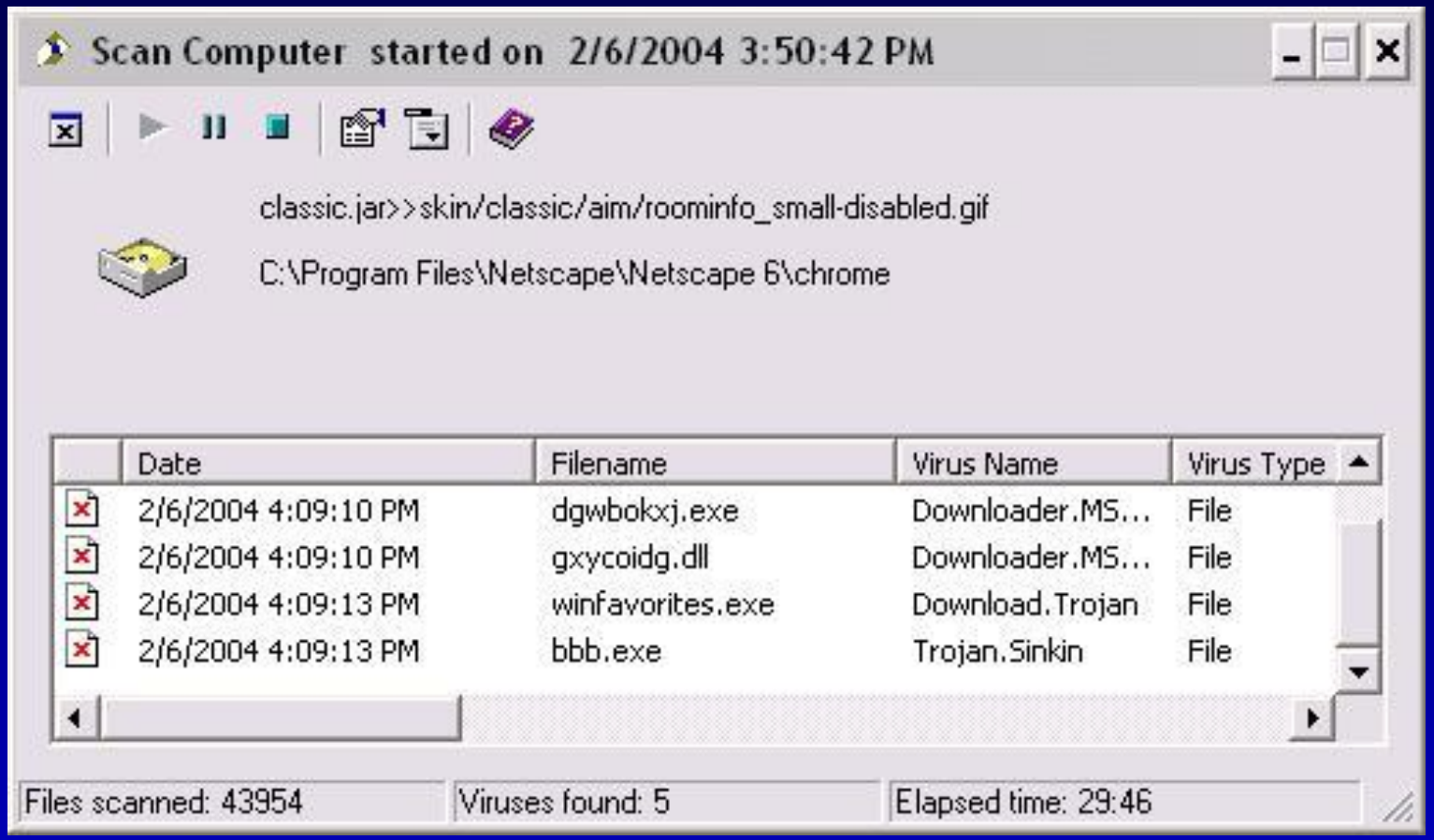
- The antivirus software updates constantly with its own server
- It gets new PROFILES of new viruses every day
- The “Scan” process enables the antivirus software to check every single file on the hard drive against the profiles
- If a file matches one of the “profiles” then it is infected, and a list is generated

Antivirus Software

- For Comcast users: Free Norton Antivirus
- AT&T: Free McAfee Antivirus (with certain plans)
- Look at taskbar, lower right side of screen
- It will alert you when viruses are detected during regular scan



Example of viruses found



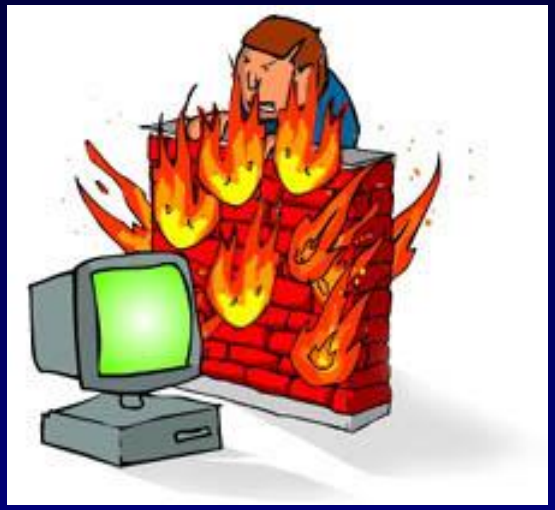
If Viruses are found, what's important?

- Make sure to tell the tech the filenames that are infected
- Make sure to tell the tech about the virus NAME
  - Knowing the name will help the tech understand the nature of the problem and how to eliminate it entirely
- HOW MANY FILES ARE INFECTED?

If A Virus Is Found, Cont.

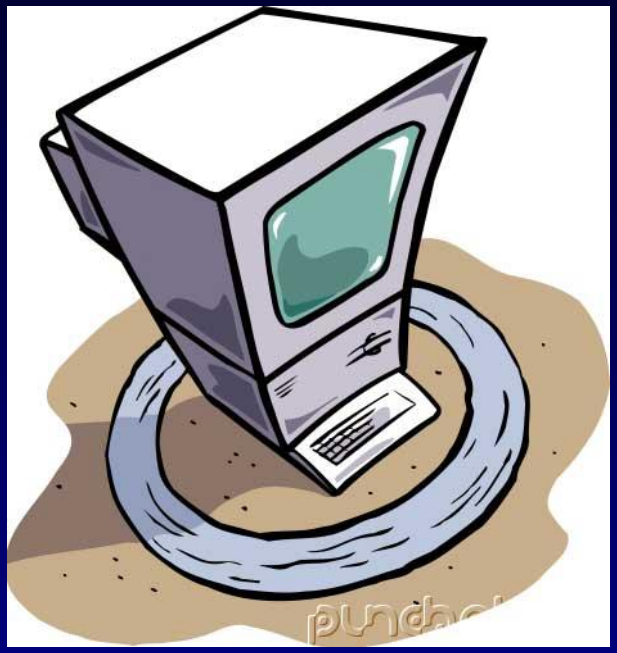
- If possible, back up any files that are saved locally on your computer
  - Make sure that you aren't backing up any of the infected files!
- Your machine may be cleanable
- Your machine may have to be reformatted
  - A tech may have to let you know if you can resurrect your machine without re-ghosting it
- Better have a backup machine (laptop, desktop, palm/pda)!

What is A Firewall?



- Acts as a gateway between you and the outside world
- Essential for broadband connections like cable/DSL
  - Continuous access=Continuous attempts to break your system!
  - Antivirus software is NOT enough
  - Windows Firewall with XP SP 2 is *ineffective*, will NOT protect you!

Firewalls Continued



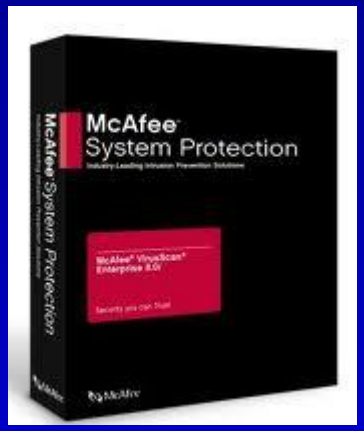
- Without a firewall, your computer=home without a door!
- With a firewall= computer is hidden or shown as locked to the outside
  - Hackers don't want to spend too much time on one system
  - "Sniffers" look for open ports on the internet. If yours is locked, hackers move on

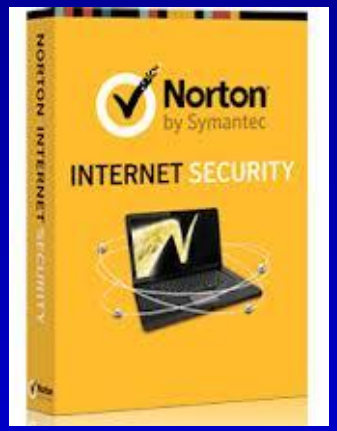
Hackers Credo

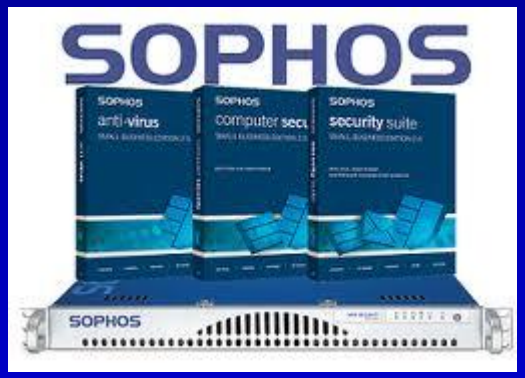
- "Always gravitate towards the path of least resistance"
- If they liked hard work they wouldn't be thieves!
- So use a firewall!
  - Like having the club on your car; Thieves may know how to disable it but it's even faster to break into a car without one!

What Is The Best Solution At Home?

- Internet Security Suites
  - McAfee, Norton/Symantec, Sophos, Barracuda, E-set, many others
    - All in one solution
    - Usually involves antispam software too
    - Parental Controls
    - Ad/Content Filtering







Policy Suggestions:

Know what you need to protect: One data breach could mean financial ruin for an SMB. Look at where your information is being stored and used, and protect those areas accordingly.

- **Enforce strong password policies:** Passwords with eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?) will help protect your data.
- **Map out a disaster preparedness plan today:** Don't wait until it's too late. Identify your critical resources, use appropriate security and backup solutions to archive important files, and test frequently.
- **Encrypt confidential information:** Implement encryption technologies on desktops, laptops and removable media to protect your confidential information from unauthorized access, providing strong security for intellectual property, customer and partner data.
- **Use a reliable security solution:** Today's solutions do more than just prevent viruses and spam; they scan files regularly for unusual changes in file size, programs that match known malware, suspicious e-mail attachments and other warning signs. It's the most important step to protect your information.

http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

- **Protect Information Completely:** It's more important than ever to back up your business information. Combine backup solutions with a robust security offering to protect your business from all forms of data loss.
- **Stay up to date:** A security solution is only as good as the frequency with which it is updated. New viruses, worms, Trojan horses and other malware are born daily, and variations of them can slip by software that is not current.
- **Educate employees:** Develop Internet security guidelines and educate employees about Internet safety, security and the latest threats, as well as what to do if they misplace information or suspect malware on their machine.

http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

What can you do to protect yourself at home?

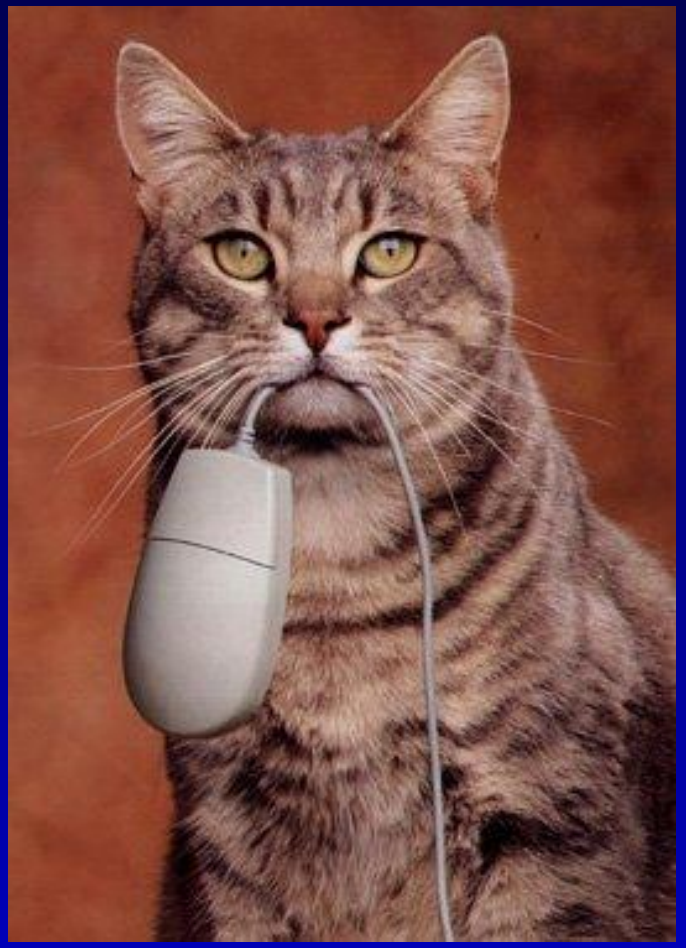
- Use up-to-date firewall/antivirus program
- Update the products when prompted
- Set an automatic download/scan time
  - SCHEDULE!
- Avoid emails w/attachments you are not expecting
  - attachments that come from FW: FW: etc.
- Avoid downloading any program that you didn't ask for

If you detect a Virus/Firewall break

- Things acting odd? Be paranoid!
- If antivirus doesn't show anything but popups still happen:
  - TRY ADAWARE(LAVASOFT), MALAWARE ANTI-MALWARE SOFTWARE, SPYBOT OR TREND MICRO'S SITE (ANTIVIRUS.COM)
- BACKUP everything you can
- Reformat system if nothing else works
  - Don't just ignore spyware!

CONCLUSION

- Being safe is a constant game of cat-and-mouse
  - Virus protection is ALWAYS reactionary
  - There is no lock made by a person that another person can't eventually open
  - Just when you think you are 100% safe is when you are the least safe!
  - Observation & Routine are the best methods to having the safest internet experiences



QUESTIONS?

How to contact

Russell Jackman, Esq.

for additional help:

Facebook.com/russelljackman

Email: **calmputerconsult@aol.com**

415-892-2617

Fax **707-220-2568**