Computer Security

A SURVIVAL GUIDE

Cory Stokes
corys@sedck12.org

Clint Stephens
clint@sedck12.org

Links in the Presentation:
http://goo.gl/w8fMH

Today's Topics

- Threats
- Safeguards
- Child Protection
- Questions & Answers

Threats

- Viruses and Malware
- Destructive Attacks
- Email Scams (Phishing)
- Identity Theft
- Privacy Violation
- Theft of Intellectual Property

What Can A Virus Do?

- There are MANY out there
- Disable security and anti-virus software if it is not detected on entry
- Allow an intruder 'backdoor' access to your system
- Steal your passwords, your personal data, your credit card numbers, your identity
- Delete files from your computer
- Send your personal files or pieces of them randomly to people in your address book
- Use your computer to send spam, store illegally copied music files or host porn sites without your knowledge
- Use your computer to participate in a 'Denial of Service' attack

Where Do We "Catch" Viruses?

- E-mail attachments
- File downloads
- Websites
- Flash Drives
- CD-ROMs

Check all files on these for viruses before opening / using!

Email Attachments

If the Email is Suspicious, do not open it!
Never click on a suspicious Attachment!

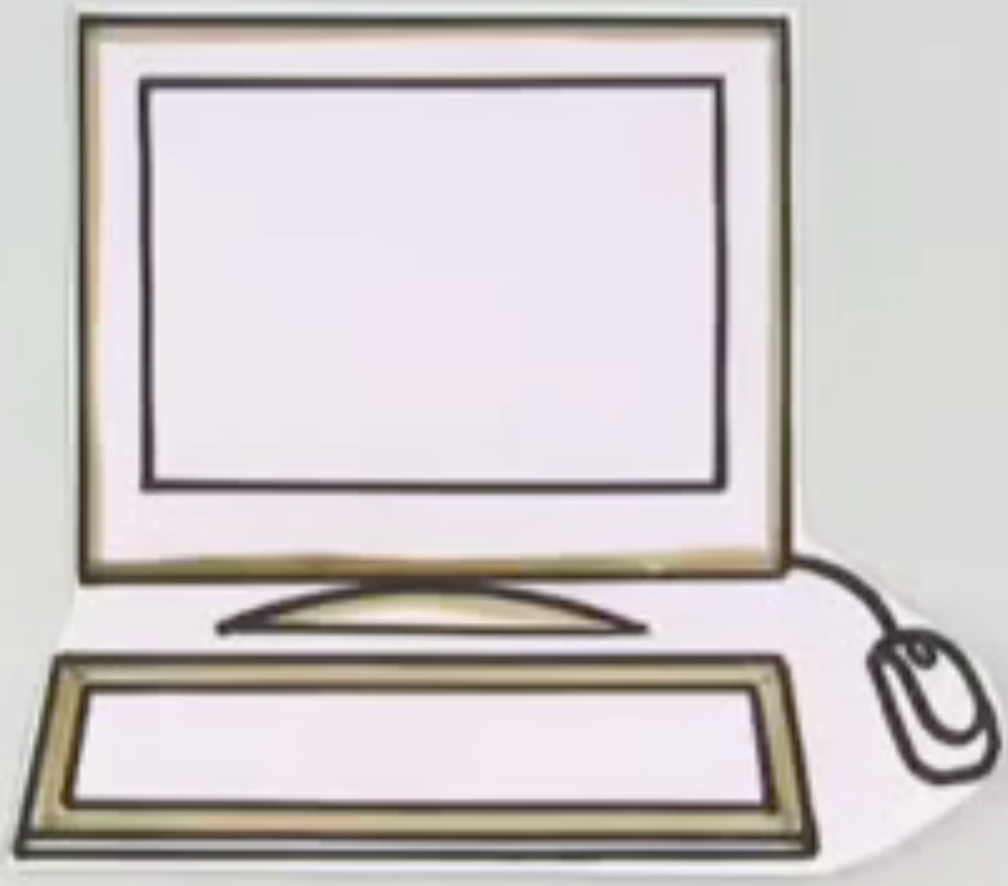
What is Suspicious?

- Message from unknown user.
- Not Work related.
- Incorrect or suspicious filename.
- Unexpected attachment.
- Unusual topic lines.

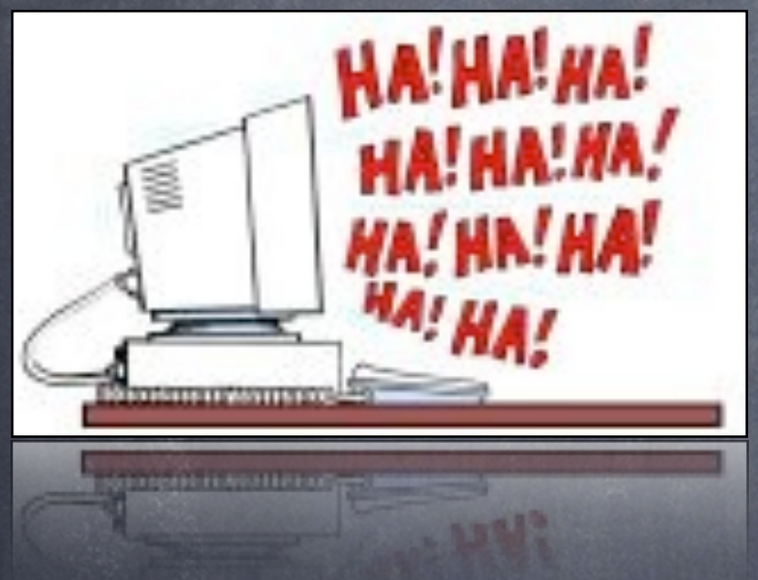
Trojans and Spyware

- Comes from companies you thought you could trust: utilities, streaming media players, "free" & "shareware" software
- Reports back to the company on what you watch or listen to.
- Circumvents corporate and personal firewalls by setting itself up as a browser "plug-in".
- May be a RAT! (Remote Access Trojan)

Phishing?



Email Scams & Phishing



- Some that may have become familiar by now: Nigerian scams
- Some that look very legit...
- Same cons as ever, just a new medium.
- Remember –if it sounds too good to be true, it probably is!
- Can lead to Destructive Attacks!
- NEVER give your personal information unless YOU initiate the contact
- Add senders to your 'Report as Spam'

Identity Theft

- "Every 45 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree." CBSnews.com
- Consumer groups estimate that as many as 950,000 people a year may be victimized by identity theft at a cost of over $46 billion dollars.
- It cost the average victim more than $1,100 to cope with the damage from identity theft, according to the FTC.
- The moral? DO NOT give out personal information unless YOU initiate the contact.

The Darker Side of Cookies

- Cookies can save information and preferences for Web sites you visit
- They can contain user names and credit card numbers that have been supplied via forms
- Cookies are used for the "targeting" of advertisements to individual users
- Programming may have security holes.
- They can also be placed by third parties – i.e. ad networks, not the site you are visiting.
- Cookies can be abused for more sinister reasons than sending 'targeted' ads –e.g. tracking your online research into controversial topics

So, Are Cookies Good or Bad?

- They are delicious, of course!
- They are not executable programs, nor are they spyware or viral - they are just informational text that a site saves to make your experience better.
- They can be labeled as a virus because they can track what you do on a site.
- Seriously, cookies are not bad as long as you have good browsing habits:
  - Don't visit Web sites that you don't trust
  - Don't give a Web site any personal information while on a public computer

Intellectual Property Theft

- Music and entertainment piracy is widespread - LimeWire and other Peer-to-Peer programs
- Not only is it illegal, but the digital format lends itself to copying and widespread distribution of files that you may not know the origin of.
- Some seemingly "legitimate" downloads could be or have spyware and virus' hiding in them - Trojans!
- Don't do this! It's not worth the numerous risks!

Software Piracy

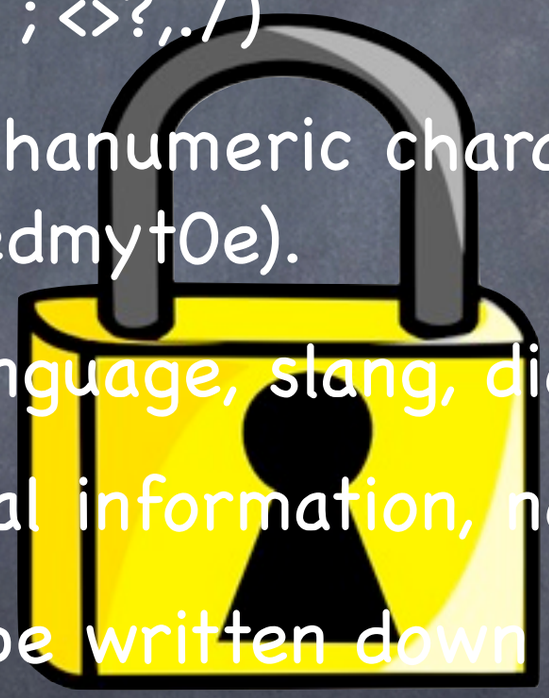
- Don't steal! There are alternatives:
- Cheaper versions –e.g. Works or Wordpad vs. MS Word
- Linux and Open Office
- Freeware and shareware products for Windows
- Google Docs
- As a bonus, you may be less susceptible to viruses which are targeted at ubiquitous Microsoft products

Safeguards

- **#1 - Keep your system patched**
- **#2 - Install and use anti-virus programs**
- **#3 - Use strong passwords**
- Use a software firewall program
- Make backups of important files and folders
- Use care & caution when downloading and installing programs
- Practice safe surfing
- Protect yourself from Identity Theft

What is a Strong Password?

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, ! @#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Are at least eight (8) alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create easy to remember passwords. One way is create a password based on a song title, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.



Practice Safe Surfing

- Be careful what information you give out
- Think before you click - Do you know the site you'll go to?
- Use dummy e-mail accounts
- Clear your memory cache after surfing, if others share your computer

Use ANY Anti-Virus Program

- Most anti-virus programs use 'signatures' or profiles to identify potential viruses
- Keep the signatures updated, preferably daily or via automatic updates from the vendor
- Set the a/v program to run in the background
- Scan any new files before opening them
- Scan e-mail messages as they arrive - many email services do this for you
- In Gmail, **View** attachments before **Download** if unsure of the origin
- Run a scan on your entire system preferably - daily (overnight), and at least weekly

Anti-Virus Program Options

- BitDefender is used in the SEDC Region
  - should be installed & running on all regional PC's
    - As a teacher in our region, you are allowed to use BitDefender on one of your home computers
    - Talk to your district Tech Coordinator to learn how to install it
- There are many options for your home computers

Keep Your System Patched

- Patches & Updates are often issued to fix security vulnerabilities
- Quick and easy to do on the PC or Mac (Yes... Mac's need patching too!)
- Use automatic updates if you trust the vendor, or set them to just notify you
- Check whether the patch can be 'undone' if it creates problems with other apps, or wait a week to see if others are having problems with it

Make Backup Copy of Important Files

- Decide which files need to be backed up
- Decide how often they should be backed up
- Decide what media to use: Flash Drives? CD? DVD? External Hard Drives? Online Storage?
- A second hard drive vs. a drive on another computer on your home network: What's safer?
- Decide where to store the backup - preferably in a fireproof container or offsite
- To be very safe, don't consider anything as "backed up" unless it is saved in 3 places

Be Smart With Passwords

- A strong password is NEVER a word found in the dictionary.
- Password 'cracking' programs love dictionaries.
- Don't use the same password for online banking or brokerage that you use for accessing content sites.
- Use different "strength" passwords for different uses.
- Easy for online newspaper accounts, but a tough one for online banking.
- Don't use the same password online as you do on your computer (if you share the computer)
- It's okay to write the passwords down somewhere safe, such as in a sealed envelope off the premises – NOT on the computer monitor!

Use Care When Installing Software

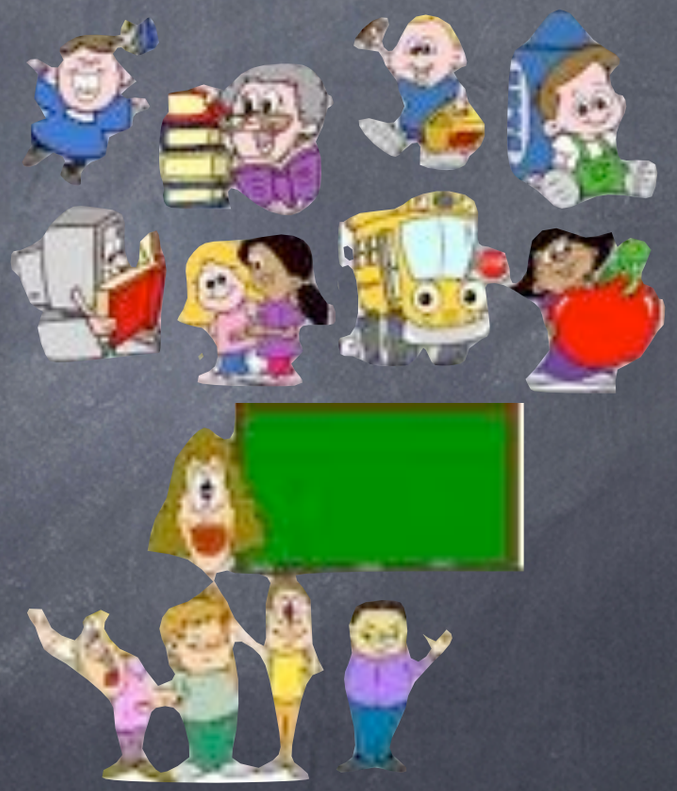
- Always follow District Policy
- First, do you really NEED the program?
- Is it purchased from a reputable commercial site? If not, was it downloaded from a reputable shareware site which virus-checks their programs?
- Beware of free lunches and 'free' software!
- Scan it with your anti-virus software

Protect Yourself from Identity Theft

- Be careful about sharing personal information – ask (yourself or who's asking) why it is needed, how it will be used, who will be sharing it, and how it will be safeguarded
- Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc.
- Don't use obvious passwords – birth dates, mother's maiden name, children name with a number after it, etc...
- Don't keep your passwords on sticky notes beneath your keyboard or worse stuck to your monitor!
- Monitor your credit rating and pay attention to your credit card and utility billing cycles

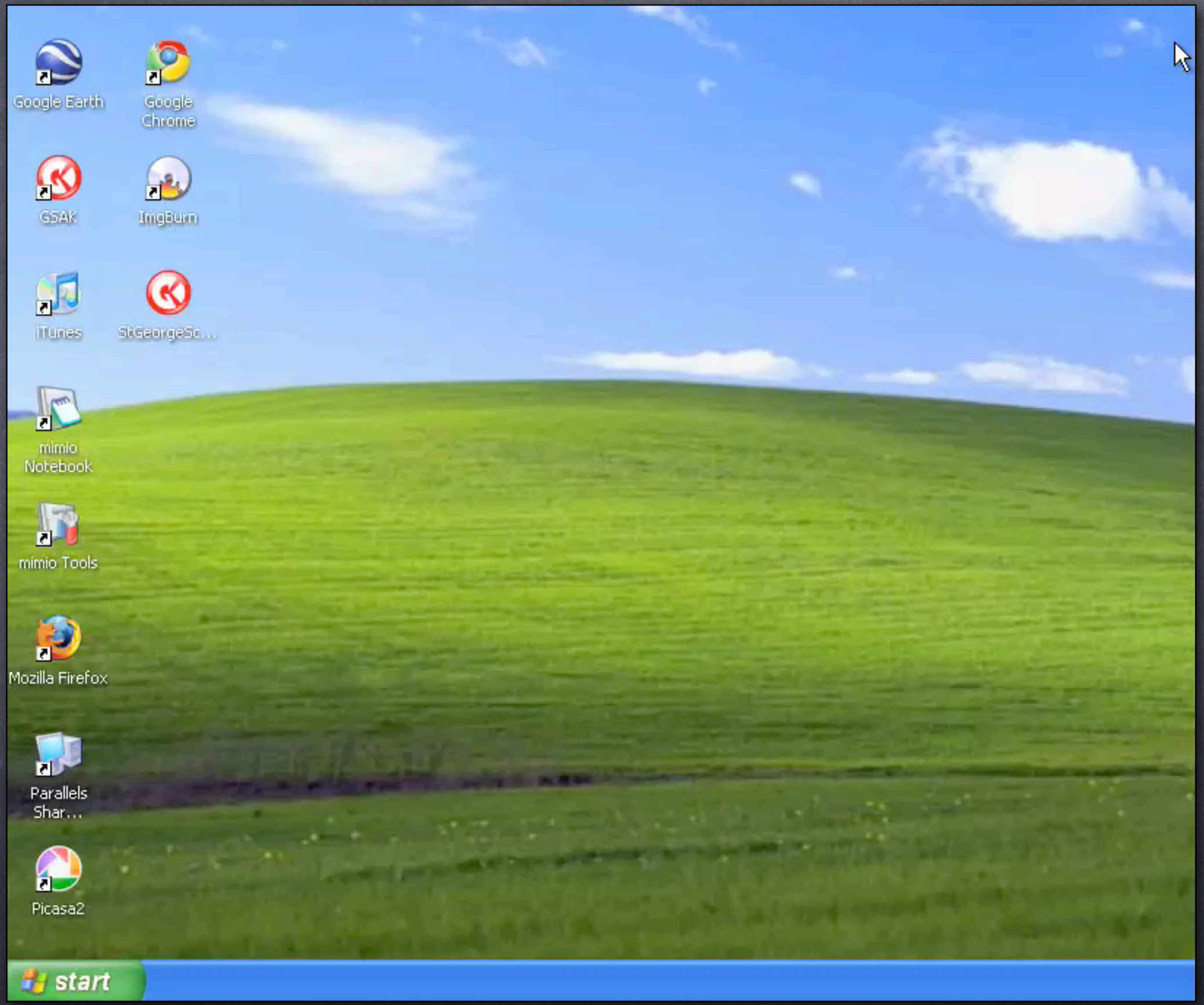
School Web and Blog Sites

- Be sure to find out and follow the Districts Acceptable Use Policy.
- Do not post personal information
- Only use Students first Name.
- Only use Photos with parents and district permission.



Summary

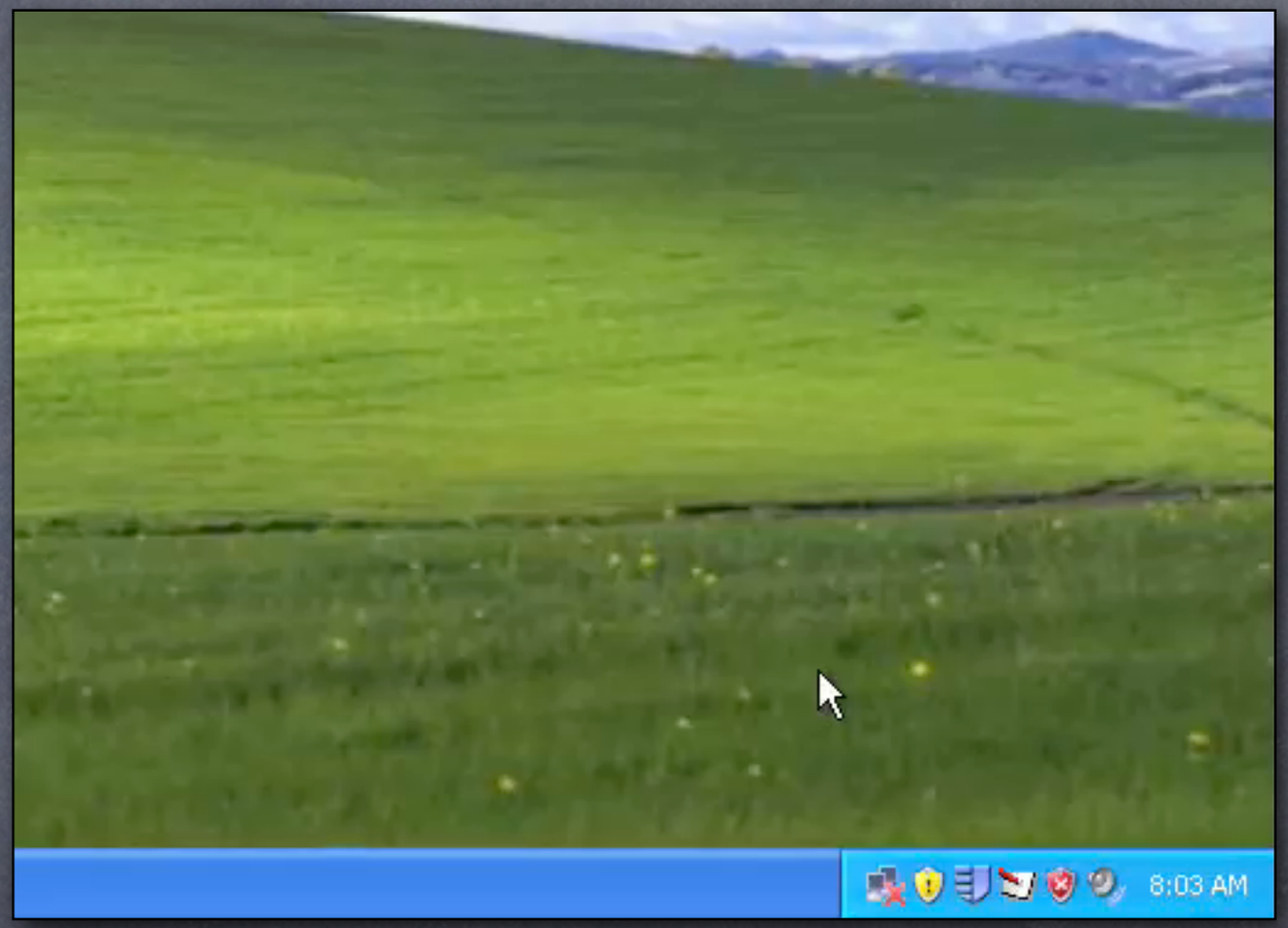
- Remember, for every online threat, some enterprising company or organization or individual has developed a safeguard.
- Use your common sense.
- Try to be cautious, not paranoid.


Google Earth
Google Chrome
GSAK
ImgBurn
iTunes
StGeorgeSc...
mimio Notebook
mimio Tools
Mozilla Firefox
Parallels Shar...
Picasa2
start

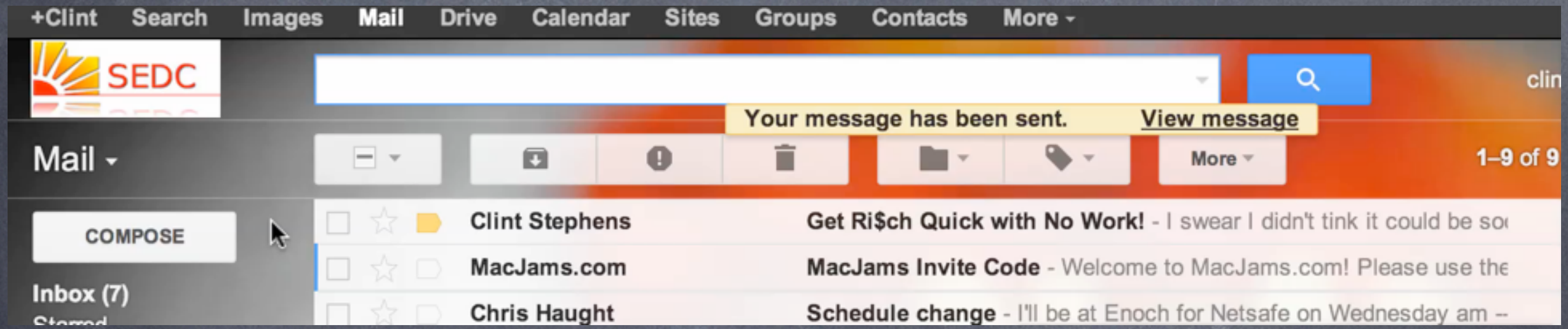
Return

Return

Return



Return


+Clint
Search
Images
Mail
Drive
Calendar
Sites
Groups
Contacts
More
SEDC
Your message has been sent.
View message
Mail
More
1–9 of 9
COMPOSE
Inbox (7)
Clint Stephens
Get Ri$ch Quick with No Work! - I swear I didn't tink it could be so
MacJams.com
MacJams Invite Code - Welcome to MacJams.com! Please use the
Chris Haught
Schedule change - I'll be at Enoch for Netsafe on Wednesday am --

Return

Virus Malware

- Dumaru
- Naith (Avril, Lirva)
- Sobig
- Bugbear
- Klez
- Conficker
- Winevar
- Nimda
- A long list...

Return

Destructive Attacks

- Distributed Denial of Service Attack (DDoS)
- Hackers 'persuade' you to let them infect your computer via e-mail, downloads or direct attack
- The hacker then uses infected computers, especially those with broadband connections, as 'zombies' to flood corporate websites with frivolous requests for access, thus depriving legitimate users of access to the site
- Targets have included Microsoft, the FBI, the White House, Network Associates, New York Times, Yahoo, CNN.com, Amazon, eBay

Return

Home Anti-Virus Options

- Sophos AV - you can install Sophos on ONE home computer.
  - talk to your local Tech Specialist for the software & necessary usernames & passwords.
- AVG Free is a good and (obviously) free solution for your additional home PC's
- There are, of course Norton AV & McAfee
  - They cost $$ plus additional $$ for updates, and are not much better
- Some options on the Mac include Intego, McAfee, & ClamXav (free)

Return