October 17, 2011

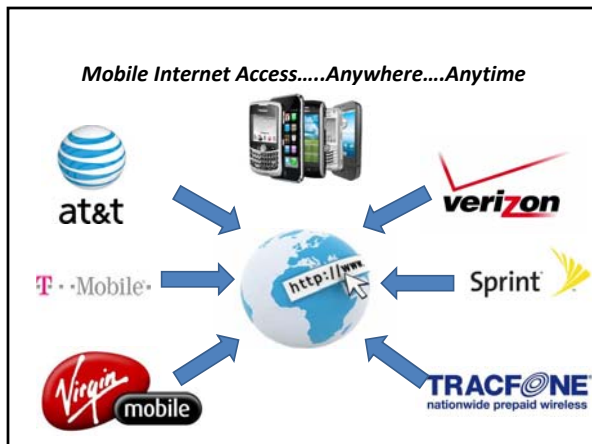*Episode I*
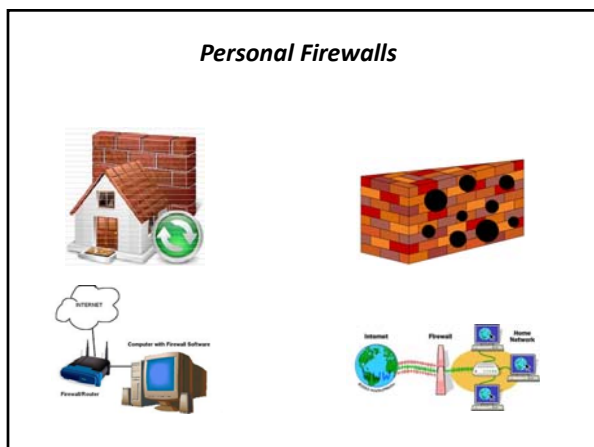
The Internet and how am I connected ….
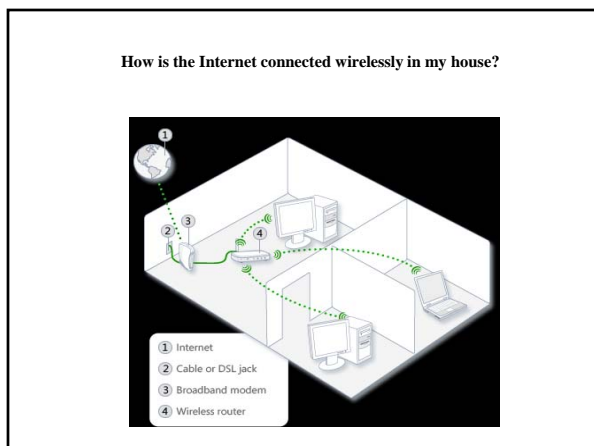
A Firewall what…….

And a Wireless whatchama call it …….
(the box with the blinking lights)

Mobile Internet Access…..Anywhere….Anytime

Home Internet Access….

at&t

Verizon FiOS

Cable Companies

Comcast

COX

TIME WARNER CABLE

DSL

Personal Firewalls

How is the Internet connected wirelessly in my house?

1 Internet
2 Cable or DSL jack
3 Broadband modem
4 Wireless router
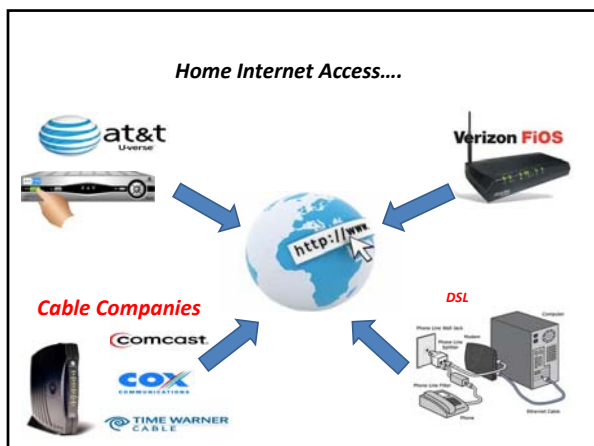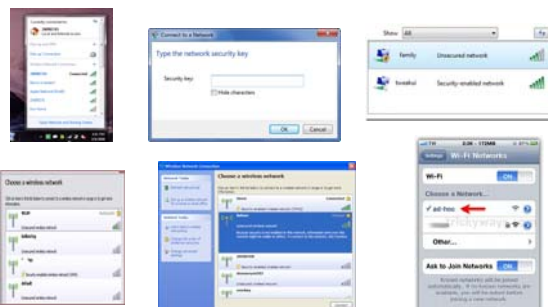
How do I know if my home wireless is secure or unsecure?

Episode II

I'm not feeling well, I think I got a cold…..no wait…maybe the flu

Maybe I picked up a virus somewhere

What do viruses do?

- Can damage files
- Can slow system
- Can show messages
- Can take control

SCAM ALERT

Hint: Review the email closely before clicking

Notice the sender's email address

Notice the printed link does not match
link when the mouse is over it......
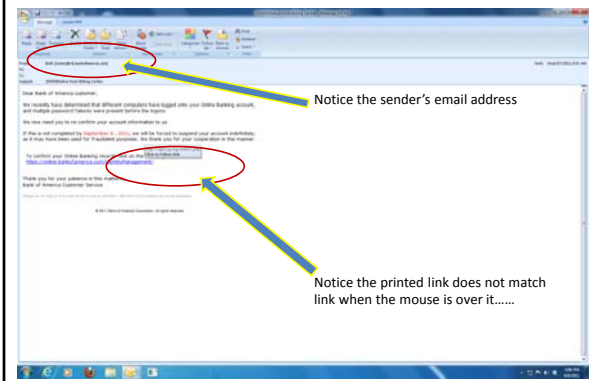
Bank of America Tip on Fraudulent E-mail

Notice 3 items:
1) Subject Line indicating urgent or alarming
2) Poor grammar, awkward or unprofessional writing
3) Misspelled words and typos
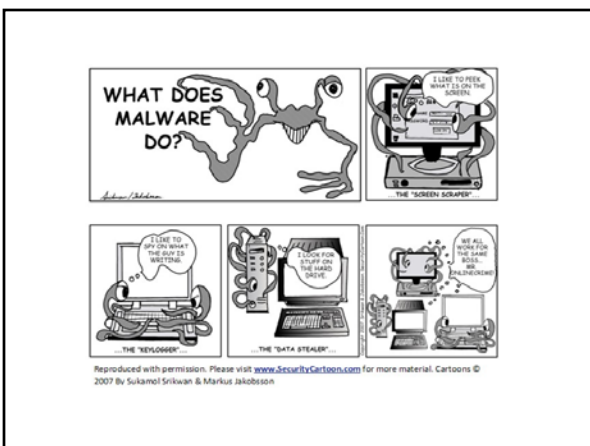
Computer Virus, Malware and Spyware….

Do I need to worry about anti-virus protection?
Yes.
New malware, and variants of existing malware, continue to circulate and present a real danger to individuals' computer systems and files. It is vital that every user take steps to protect themselves and their systems; if you fail to do this you are risking not only your own computer but other computers in your household.

What should I do if I think I have a virus or other malware?
Don't panic.
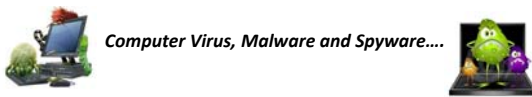There are thousands of pieces of malware, each with its own mode of attack. Many infections result only in inconvenience and loss of time; an infection does not necessarily mean you are going to lose important files or damage your computer.
If your computer begins to behave strangely, e.g. run very slowly, bleep without reason, lock up or crash, display bizarre messages, or if your documents become corrupt or contain text you didn't type, these may be symptoms of malware, although they can also arise for a host of other reasons. On the other hand, some malware just spreads through your system with no outward sign. The only way to discover whether you have a virus or other malware is to scan your system with up-to-date anti-virus software that may be able to detect and remove the virus/malware

---

How do I protect my system?

1. Ensure that you have up-to-date protection software

2. Don't open any email attachment you are not expecting to receive, even if it appears to come from a friend (in general you cannot acquire malware just by reading the main text of a mail message, unless your patching is very out of date). Note that attachments purporting to be security updates from Microsoft are hoaxes and should never be opened.

3. Don't go to a link included in an email. In particular, for anything where money is involved, e.g. your bank, eBay, PayPal, use a bookmark you have previously saved.

4. Don't follow a link in an unexpected message in an instant messaging client, even if it appears to come from someone on your friends list; malware is designed to exploit trust.

5. Don't accept and use unsolicited media, e.g. DVDs, CDs, ZIP disks (even disks on magazine covers have been known to contain malware)

6. If you are doubtful about a disk, file or attachment, but think it may contain something you want, you can check it using your anti-virus software - this is not foolproof however, since the malware writers do their best to keep one jump ahead of the anti-virus/malware developers.

7. Don't run programs or open documents (e.g. Word/Excel) whose origin you don't know.

8. Some protection against macro viruses is offered by turning off macro execution in Word or Excel (keep the SHIFT key down when opening a document).

9. If in doubt about any of the above, ask someone who knows or can assist you.

10. Maintain regular backups of all important material on your computer, in case you ever need to recover from a major virus infection or any other disaster.

How do I know if I have Spybot and Malware software installed ?

Both Spybot and Malware have the same type of icons

Prescription?

Antivirus Software:
- AVG
- AVAST
- BitDefender
- ESET
- Kaspersky
- McAfee
- Norton
- Panda
- Sophos
- TrendMicro
- Zone Alarm

Free Antivirus Software:
- AVG
- AVAST

Dosage:
Minimum – Weekly
Best result – Daily*

* Since viruses can change hourly, the best would be to update and scan daily. If you cant, then a minimum would be to update and scan your computer weekly.

Malware:
- MalwareBytes
- Spybot Search and Destroy

Resources

Antivirus Software:
- AVG – www.avg.com
- AVAST - www.avast.com
- BitDefender - www.bitdefender.com
- ESET – www.eset.com
- Kaspersky - www.kaspersky.com
- McAfee – www.mcafee.com
- Norton – www.norton.com
- Panda – www.pandasecurity.com
- Sophos – www.sophos.com
- TrendMicro – www.trendmicro.com
- Zone Alarm – www.zonealarm.com

Free Antivirus Software:
- AVG – www.avg.com
- AVAST – www.avast.com

Malware:
- MalwareBytes – www.malwarebytes.org
- Spybot Search and Destroy – www.safer-networking.org

What about my children and Internet access?

Free Web Monitoring Software

http://www1.k9webprotection.com/

What about Social Networking sites?

Your kids are on Facebook. Keep them safer with SocialShield.

Comprehensive Alerts

We alert you to a range of safety risks including cyberbullying and predators as well as talk of drugs, alcohol, violence or sex that could damage your child's reputation or represent a potential threat.

360 Degree Monitoring

Unlike traditional parental control software, SocialShield instead constantly watches social networking activities regardless of what computer or phone is used to connect to the network, and provides warnings and alerts of potentially concerning or threatening activities which you can then review, saving you countless hours of work.

http://www.socialshield.com/   *Note: There is a monthly fee for this service*

Passwords…..

Password-cracking software tools continue to improve, and the much more powerful computers we have today only assist them. Some password-cracking tools use dictionary attacks. They simply try a list of words—such as, for example, commonly used English words and names.

In addition, there are automation-type tools that try every possible combination of letters and other characters. Given enough time, the automated method can crack any password. Consequently, passwords that once took weeks to break can now be broken in hours by the best cracking tools on a fast computer. So you need to get more crafty and cunning.

You have to pick a password that is hard to break because it isn't obvious or hackable. This is called a "strong" password. For a password to be strong, it should meet the following criteria:
- Not be a common word or name
- Not contain your name or your computer-user name
- Be significantly different from any passwords you have used previously
- Be at least seven characters long—and longer is even better
- Contain at least one character from each of the following four groups:
- Uppercase letters (A, B, C …)
- Lowercase letters (a, b, c …) Numerals (0, 1, 2, 3 …)
- Symbols, meaning all characters not defined as letters or numerals (including ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /)
- Have at least one symbol character in a position other than the first and last spot

SHOULD I CHANGE MY PASSWORD

Is your password easy as 123?

Passwords…..

Intruders attempt to gain access to shared computer systems through the accounts of others. Their motives vary from curiosity to criminal malice. At risk are:

Your files. An intruder can steal, modify, or destroy the information you keep on the shared computer. The privacy of your e-mail is also at stake.

Your reputation. An intruder can send slanderous, defamatory, or otherwise embarrassing e-mail from your account, under your name. An intruder could also store material on your account that would implicate you in illegal or unethical acts.

Your financial security. An intruder can gain access to your financial information.

Resource Link:
http://news.yahoo.com/blogs/upgrade-your-life/upgrade-life-5-ways-easy-remember-ultra-secure-205840345.html

Password Challenge Questions… What you are starting to see in banks….

Security Question

Change your security question and answer as needed. The security question is used to verify your identity if you have forgotten your password.

Authentication Security Question*

Who is your favorite singer?

Who is your favorite childhood hero?
What is name of your favorite restaurant?
Who is your favorite actor?
Who is your favorite singer?

In what year (YYYY) did you graduate from high school?
Answer:

(Not case sensitive)

Forgot the answer to your SiteKey Challenge Question?

Episode III

What do I do….?

Well..it looks like your on the Internet already

1. Google yourself and see what's already out there
2. Check yourself out at www.spokeo.com
3. How about www.zabasearch.com
4. Then there is www.zoominfo.com
5. Oh, and www.pipl.com
6. Of course there is www.peoplefinders.com
7. Don't forget www.people.yahoo.com

Google

pipl.com

spokeo

ZABASEARCH
Free People Search and Public
Information Search Engine

YAHOO!

AnyWho
Part of the new at&t

zoominfo
find people and companies

peoplefinders
find anyone, anywhere

Just for fun….
Can you tell what is common between these objects?
How about what is different between the mailboxes?

What's in your mailbox…….

Ms. Jane Doe

World Wide Web

Ms. Jane Doe

Paper documents at home…….

What information do they contain?

Credit Card bills
Gas Card Bills
Department Store bills

Best way to destroy them…..Cross cut shredders available at:
• Staples
• Office Depot
• Office Max

Secure Mailboxes

FRONT VIEW

What to do then…..

How can you find out if your identity was stolen?
The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done:
- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

What should you do if your identity is stolen?
1. Filing a police report
2. Checking your credit reports
3. Notifying creditors
4. Disputing any unauthorized transactions

Resource link:
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html#Howcanyoufindoutifyouridentitywasstolen

---

October 2011 Issue of Kiplinger's Personal Finance

LIVING

What You Need to Know About Getting Hacked

Cyber crooks are becoming more brazen. But you can take simple, effective steps to fend off attacks.

Do you have a AAA membership?
If so, AAA offers free credit monitoring.
Check with your local AAA office

Resource Document

TAKE CHARGE:
Fighting Back Against Identity Theft

Resource Document

- If Your Personal Information Has Been Lost or Stolen 4

ID THEFT VICTIMS: IMMEDIATE STEPS 5
- Placing Fraud Alerts on Your Credit Report 5
- Closing Accounts 7
- Filing a Police Report 8
- Filing a Complaint with the Federal Trade Commission 8
- The Identity Theft Report 9
- Tips For Organizing Your Case 10
- Chart Your Course of Action 11

RESOLVING SPECIFIC PROBLEMS 12
- Bank Accounts and Fraudulent Withdrawals 12
- Bankruptcy Fraud 17
- Correcting Fraudulent Information in Credit Reports 17
- Credit Cards 19
- Criminal Violations 20
- Debt Collectors 21
- Driver's License 22
- Investment Fraud 22
- Mail Theft 23
- Passport Fraud 23
- Phone Fraud 23

Additional resources

http://www.idtheftcenter.org

http://www.howstuffworks.com/identity-theft.htm

http://www.ftc.gov/bcp/edu/microsites/idtheft

http://fraudwatchinternational.com/identity-theft/idtheft-victim-help

Equifax: 1-800-525-6285; www.equifax.com
P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (1-888-397-3742); www.experian.com
P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA
92834-6790

Disclaimer: Neither the presenter nor its organization endorses or supports the presented software company. The information is provided to you as a resource and the individual will need to make their own determinations as to the value of the information.

Questions ???????

Contact Information:

Carl Fong
Executive Director Information Technology
Orange County Department of Education
Email: cfong@ocde.us
Phone: 714-966-4185