



THE AIDS
LIBRARY



CRITICAL PATH AIDS PROJECT

Critical Path Project Internet Services Security Manual

A guide to safety on the Internet, email, and your home computer

Surf the Web safely • Email without worry • Protect your computer

For More Information visit:

www.critpath.org

Philadelphia FIGHT
1233 Locust Street
Philadelphia, PA 19107
215-985-4851

Every day we put ourselves at risk while using computers!

But computers are part of everyday life....

So how do we protect ourselves?

HOW AM I AT RISK?

We use computers every day for so many simple tasks. Sometimes, we don't realize that we may be targets for people who will take advantage of our inexperience or lack of security.

Both our PERSONAL safety and our COMPUTER'S safety may be compromised when we use the Internet.

Personal Safety

When using computers, we can put our personal safety at risk in the following ways:

- We may reveal personal information to strangers
- We may suffer harassment or be involved in uncomfortable interactions
- We may have our identity stolen
- We may put ourselves in financial danger
- We may even put ourselves in physical danger

Computer Safety

When using computers, we can put the machine at risk for the following:

- Viruses can cause damage to our computers
- Hackers and snoopers may directly invade our computers
- Even friends or family may have information that may put our computers in danger

IMPORTANT:

All risks associated with computers are related to using the Internet, using Email, or using Disks/CDs in multiple computers!!!

Read more to find out the specific risks and how you can become a smarter, savvier computer user!

PERSONAL SAFETY SURFING THE WEB

Every time we surf the World Wide Web, we put ourselves at risk. Many websites we visit collect information about our computers and about how we surf the Web. Other websites may insert programs onto our computers without us knowing it!

The following are the most common problems encountered when surfing the Web.

Risk #1: Pop-up Advertisements

These pesky ads often pop up on legitimate websites that we are visiting. They come in all shapes and sizes. Some are helpful. For example, an HIV website might have an ad from a specialty bookstore where you can purchase books or materials related to HIV.

BUT many of these pop-up ads are SCAMS. Once you click on them, they lead you away from where you are. Often these ads will download something to your computer, such as an unnecessary toolbar or even a pornographic image or website!



According to CNET News.com, the company Bonzi is at the center of a lawsuit for their ads that FALSELY state messages that say, " the words **"Security Alert," "Message Alert" or "Warning."** One such banner reads: **"Your computer is currently broadcasting an Internet IP Address. With this address someone can immediately begin attacking your computer."** If surfers click on the X to close the banner, they're delivered to Bonzi's Web site."

These ads can also collect the IP address of your computer (this is the virtual location of your computer). Once they have that, they can track your movements on the Internet.

What You Can Do:

- ① Learn to recognize ads on a website.
- ① Only click on those ads that seem like they might be helpful.
- ① Don't download anything, unless you have checked out the company
- ① Don't believe what ads tell you! They are trying to sell you something!

Risk #2: Cookies

Whenever you go to a place like Amazon.com or Columbiahouse.com, you can create a profile for yourself and store prospective items in a "shopping cart." These websites will install a **cookie** onto your computer to help remember the information you gave them. Next time you visit the site, you won't have to type in your password and all of your selected items will still be in your shopping cart.

Cookies are small pieces of information that are stored on your computer, and ready for websites to access when needed. This sounds like a great idea. Many cookies are harmless.

BUT, cookies are also a way for these websites to keep track of your movements. These websites gather information from your computer and then send targeted advertisements to you. Others will release information they have collected to other companies that you may not want to have your information.

Finally most websites don't tell you when they install a cookie on your computer, so you don't know when it is happening!

What You Can Do:

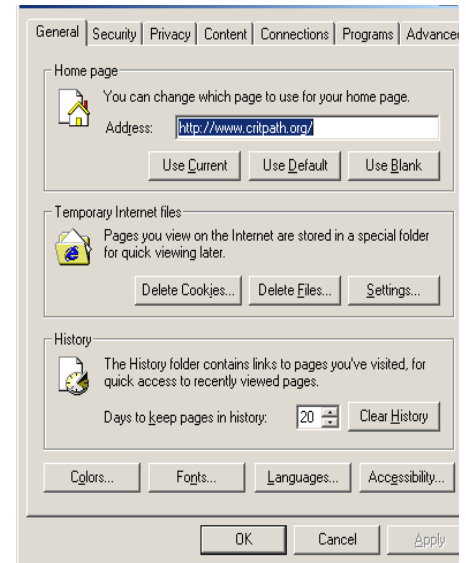
① Delete your cookies once a day or once a week!

- ① In Internet Explorer, go to "Tools"
- ① Go to "Internet Options"
- ① Under "General," click on "Delete Cookies"

① Disable cookies completely.

–NOTE: if you do this you may have trouble online shopping.

- ① In Internet Explorer, go to "Tools"
- ① Go to Internet Options
- ① Click the tab "Security"
- ① Highlight the icon "Internet" and select "Custom Level"
- ① Select "disable" under "cookies" (internet explorer) – doesn't use cookies!



Risk #3: Online Shopping

You now know how cookies are used in online shopping. When you shop online, you have to provide more information than if you simply shopped at the mall. Online shopping sites ask for your address, phone number, email address, and, of course, your credit card information.



Always making sure the site is legitimate BEFORE you give out your credit card info! Many sites may seem legitimate, but because they are online, it is difficult to tell.



Stolen financial identity *is* a risk. With little more than your name and credit card number, someone can literally "steal" your identity and spend thousands of dollars in your name. Be careful where you type your personal and financial information on the Internet.

What You Can Do:

- ① Never deal with a company that does not provide its address and phone number on their website
- ① Never shop at a company that does not have a privacy policy.
- ① Make sure the website you are shopping at is *encrypted*. This means that it is a secure site. An encrypted site has a little padlock icon located at the center right bottom of Internet Explorer and at the bottom left of Netscape Navigator.
- ① Never buy anything from an unsolicited email or SPAM!



<http://www1.eckerd.com/content.asp?content=help%2Fpolicies%2Fsecurity>

CHATTING AND MEETING PEOPLE

One of the most fun activities on the Internet is being able to chat and connect with people around the world.

Chat Rooms and Internet Dating are a great way to meet people but both have risks.

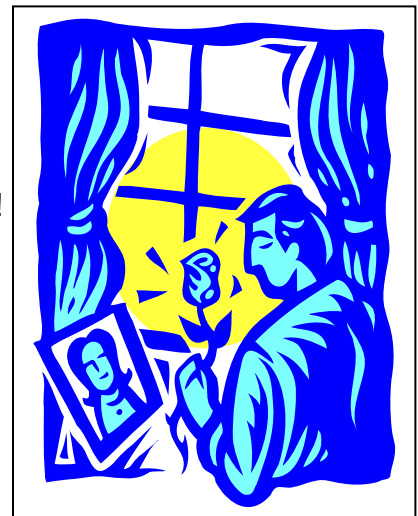
Risk #4: Internet Dating

Want to meet that special someone?

Well, many have found love over the Internet. Others have gotten stuck with huge fees and lots of creeps. Many online dating sites do not screen people who join their groups. That means anybody can join and **pretend** to be whoever they like!

Over the Web, many people have fake personas. If you are looking for a 35 year old man, make sure he is not a 13 year old boy playing a joke.

It is up to you to be careful about how much information you reveal to that potential date. Exercise your best judgment.



What You Can Do:

- ① Never reveal your last name, personal website, home address, or phone number until you are ready.
- ① Stop communicating with someone who pressures you to reveal information.
- ① Use a different, anonymous email address than your regular one.
- ① Use a phone number that is not listed, like a cell phone number.
- ① Talk on the phone first.
- ① **Always meet in a public place for the first time!!** Do not have anyone pick you up at your home.
- ① Let a friend/family member know where you will be on a first date.
- ① Request a photo if one has not already been provided by the dating service.

- ① Be aware of inconsistencies in information that is given to you or failure to give direct answers.

Risk #5: Chat Rooms

Like Internet dating, chat rooms can be a great way to meet people and talk about your favorite topics. Chat rooms may have few or no rules, so they can be a haven for deception!

Teenagers often love chat rooms but parents should monitor whom young people are speaking with and which chat rooms they enter. It is very easy to deceive someone in a chat room and everyone should always be a guard when chatting.

The same guidelines for Internet dating should also be followed when you are in a chat room.

Some cyber-stalkers will set up a website and only reveal the web address with whomever they are chatting. Once you go to their website, you are the only one who has hit the website, and they can capture your IP address. Once they have your IP address, they are well on their way to tracking you down.

What You Can Do:

- ① **Never reveal personal information!** This can include your sex, age, school, city, favorite sports team, etc... With a little bit of info, you can easily be found.
- ① Never use your real name or a nickname that everyone knows you by.
- ① Do not give out your email address, website, or phone number.
- ① If you are planning to get together with someone you met in a chat room, always pick a public meeting spot.
- ① Leave a chat room immediately if anyone makes you uncomfortable.
- ① Be aware of entering into a private chat room. People will take advantage of the one-on-one chat to make harassing or inappropriate remarks.
- ① Many chat rooms have guidelines for appropriate behavior. Only use chat rooms that provide a policy and their contact information in case you are harassed.

Risk #6 Instant Messenger

AOL, MSN, Yahoo – these are the most frequently used forms of Instant Messenger. Like chat rooms, you can send and receive messages to whoever is currently on Instant Messenger in real time. Instant Messenger programs make you feel as if you are having a conversation directly with someone.

All of the precautions used in chat rooms should be followed whenever using an Instant Messenger program! Remember, they are:



- ① **Never reveal personal information to anyone who you do not know!**
- ① Don't use your real name or a nickname.
- ① If planning a face-to-face meeting for the first time, always meet in a public area.
- ① Do not give out your address, phone number, email, or website.

COMPUTER SAFETY

COMPUTER VIRUSES



Hal Mayforth:
<http://www.mayforth.com/illustration/virus.htm>

Everyday the computers that you use risk being attacked by people out there on the Internet trying to cause trouble. These people create viruses and other computer programs that can cause a lot of damage to your computer.

What is a Computer Virus?

Computer viruses are small programs that spread from one computer to another through email or by using disks in different computers. These programs can damage your computer and information you have on your computer, and can even send themselves to other people using your email address.

How do I know I have a computer virus?

Here are some clues:

- ① Your machine runs at a snail's pace, or it frequently shuts down.
- ① You get messages that you have no memory left
- ① Your data starts to disappear before your eyes and you have not hit delete.
- ① Files and documents aren't where you saved them or you can't open them
- ① Strange sounds or images play on your computer
- ① You begin to type and strange objects appear instead of characters.

IMPORTANT!

Sometimes, you may not realize you have a computer virus at all! Many computer viruses give no sign of their presence, so it is important to protect your computer now.

EMAIL SAFETY

If you use email now, you probably wonder how you ever got along without it. It is easy, fun and convenient. But email can also carry a lot more than friendly messages.

Risk #7 Attachments:

Email attachments like videos, sound clips, and documents are also great to send to others. But, email messages can carry computer viruses that are activated simply by opening an email attachment. They will infect your computer and possibly the computers of all the people listed in your contacts or Address Book.

What You Can Do:

- ① NEVER open an email attachment from someone you don't know.
- ① Delete any email that seems suspicious or seems to have a suspicious attachment.

Risk #8 Spam:

Spam is junk mail. Just as you probably receive a lot of junk mail at home, you can also receive junk email to your email address. Spam emails advertise get-rich-quick schemes, dangerous diet or vitamin pills, and other dubious products. Spam messages may contain links that when clicked on, lead to a website that will download a virus.



They can also lead to a website that will capture your IP address or install a cookie. And finally once you click on the link, they can confirm that your email address is active and they will continue to send you junk mail!

Spammers get your email address many different ways:

- Many online stores sell lists of customers' email addresses to spammers.
- They also steal email addresses from online chat rooms or discussion boards.
- They even try to guess email addresses and send messages to likely addresses (maryjane1@aol.com, maryjane2@aol.com, etc).

What You Can Do:

- ① Use an email filter. In Critical Path you can "blacklist" certain addresses from sending you mail.
- ① Use an unusual email address (zbrr2w9@critpath.org for example).
- ① Be careful giving your email address to a website (ex: during online shopping). Read their privacy policy before giving your address to any website.
- ① When you do give your email address to a website, *uncheck* any check boxes for free newsletters or special offers – websites often check them in for you.
- ① Don't list your email in chat rooms or bulletin boards.
- ① Don't post your email address on a public website, like eBay
- ① Never buy something from a spam email. Even if the offer isn't spam, you can get bombarded with more spam.
- ① Don't forward chain letters, petitions, or virus warnings. Spammers use these to get email addresses.
- ① Report spam to the Federal Trade Commission (they are trying to reduce spam) by forwarding it to spam@uce.gov
- ① Send a complaint through postal mail to a company that sends you spam often.
- ① Use multiple email addresses – one for friends and family, one for online shopping or bulletin boards, etc.
- ① When you start getting too much spam in an email address, stop using it and start another email account.

Risk #9 Phishing:

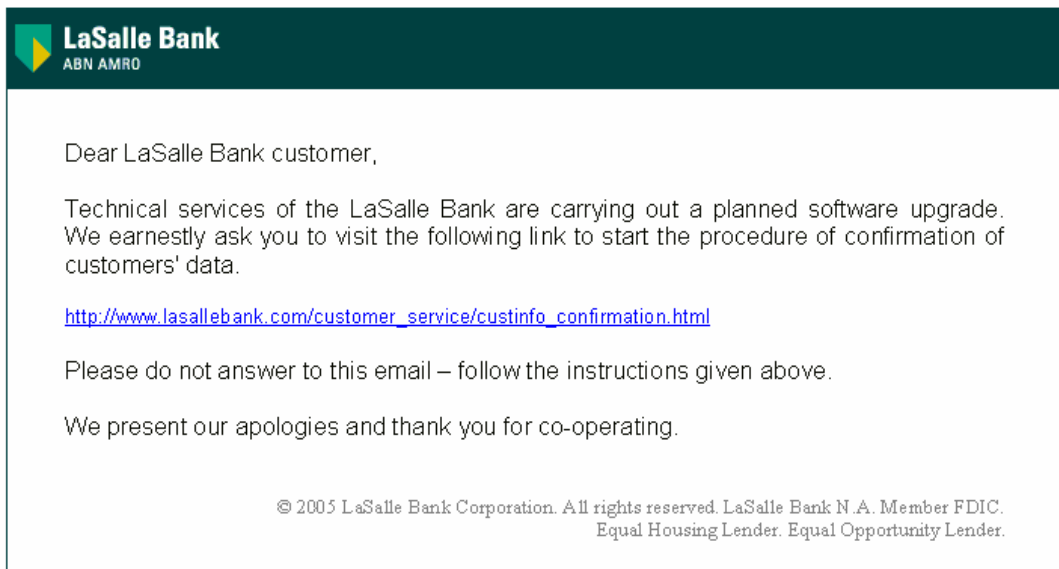
Phishing is when you receive spam that attempts to lure personal information (including credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from you.

Phishers send an email message that claims to be from a business or organization that you may deal with — for example, a bank, an online store, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond.

The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

From: LaSalle Bank

Subject: Attention To All LaSalle Bank Clients



What You Can Do:

- ❶ If you get an email that asks for personal or financial information, do not reply. And don’t click on the link in the message, either.
- ❶ Contact the company, bank, or organization directly if you are unsure if an email is legitimate or not.
- ❶ Ignore emails from a company, bank, or organization that mentions your account but address you as “Dear Customer” or “Dear Client.”
- ❶ Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email.

DISKS, PASSWORDS & VIRUS SOFTWARE

Risk #10 Computer Disks:

Since you may not even know you have a computer virus on your computer, you can easily spread it to other machines.

FOR EXAMPLE: you may be writing a Word document and decide to copy it to a computer disk. You don't know that the document is infected with a virus. You then use the computer disk in a friend's computer. This computer is now infected with the computer virus from your computer!

The best way to protect your computer and your disks is to use Anti-Virus Software.

What You Can Do:

- ① Always save your work in more than one place -- on disk and on your computer.
- ① Use **Anti-Virus Software**, such as Norton Antivirus or McAfee. These programs charge a minimal yearly fee. (Free software includes AVG Anti-Virus System at www.grisoft.com and Anyware Antivirus at www.helpvirus.com)
- ① Regularly update your anti-virus software! Virus software only works if you run the program at least once a week.
- ① If your computer is infected, take action immediately. If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with fully updated anti-virus software.
- ① Use your computer's security features
--In Internet Explorer, go to: Tools/Options/Security/Custom Level - High

Risk #11 Passwords:

A good password prevents other people from entering your online accounts and keeps you and your computer safe and secure.

Think about the password for your email address, online shopping accounts, chat room sign-in, and any other place on the internet you have to log-in. Spammers and those looking to cause trouble on the Internet could easily break into your online account and infect your computer with viruses or steal financial information.

What You Can Do:

- ① Use passwords that are hard to guess – they should include at least 4 letters and two numbers.
- ① Don't use:
 - Your first or last name
 - Your child or spouse's name
 - Information about you – your street, your phone number, etc..

- A word that you could find in an English or foreign language dictionary
- A password less than 6 characters
- A password of all the same numbers or of all the same letter
- ① Use a password that is easy to remember, so you don't have to write it down.
- ① Use a password you can type quickly, so that it is hard for someone to steal your password by looking over your shoulder

Tricks to making up a great password:

- ① Choose a line or two from a song or poem, and use the first letter of each word. Example: `` It's been a hard day's night" would be "ibahdn".
- ① Alternate between consonants and vowels, up to eight characters. This creates nonsense words that are usually pronounceable, and easily remembered. Examples: ``routboo," or ``quadpop."
- ① Choose two short words and join them together with a punctuation character between them. Example: ``dog+F18' or 'comP7UTer'.
NOTE: 'dog', 'F18' and 'computer' are in dictionaries but because these passwords use punctuation or digits they are really hard to guess.

THE LAST LINE OF DEFENCE: FIREWALLS

Every time you go on the Internet, you and your computer are at risk. Even with anti-virus software, individuals can still attempt to hack into your computer and gain access to your information.

Turning off your connection to the Internet when you are not using it is the only sure-fire way to keep hackers out. This is particularly important for those who are using DSL or Cable Internet access, which is "always on" even when your computer is off unless you turn the Internet connection off.

A firewall can help prevent hackers. A firewall is a program that creates a fence around your computer, blocking any unauthorized users from accessing your system.

Personal firewalls are used for home computers and cost anywhere from nothing to \$50 or so. Windows XP comes with a free firewall ready on the systems. Some anti-virus software also comes with a firewall upgrade. Other programs are free!

What You Can Do:

- ① Purchase or download a firewall. Check out these recommended free firewalls:
 - ① ZoneAlarm <http://www.zonelabs.com/store/content/home.jsp>
 - ① Kerio Personal Firewall http://www.kerio.com/kpf_home.html
 - ① Outpost Personal Firewall <http://www.agnitum.com/products/outpost/>
 - ① Sygate Personal Firewall http://smb.sygate.com/products/spf/spf_ov.htm
- ① Make sure you run the program frequently.
- ① **Always** use a firewall when using file-sharing programs such as KAZAA, Morpheus, or Grokster.

There is always more to learn about your personal safety and computer security. A glossary, resource list, and top 10 things you can do is available. The most important step is being aware of the risk and not letting others take advantage!

You are now well on your way to being well-informed on cyber safety!

Good Luck, Stay Safe, and Have Fun!

Contact the Critical Path Help Desk for any Critical Path problems:

| | |
|--|--|
| <p>Our Hours are: Mon. -Wed., Fri. 9 am-5 pm Thurs. 9 am-8 pm 1233 Locust Street, 2nd Floor Philadelphia, PA 19107 Phone: (215)985-4851 x140 Fax: (215)985-4492 Email: library@aidslibrary.org Website: www.critpath.org</p> | <p><i>Critical Path is a free service, please do not abuse it.</i> Critical Path provides technical support during office hours. Call, email, or fax your questions, and we will respond as quickly as possible. The Critical Path AIDS Project and the AIDS Library cannot provide onsite technical support at your location. The AIDS Library uses and recommends Yikes, Inc.; a fee-based technical support service.</p> |
|--|--|

GLOSSARY

Anti-virus software

A program that scans your computer for computer viruses. The software needs to be updated regularly in order to protect your system from new viruses discovered every day.

Attachment

A computer file (like a picture or a document) that is sent along with an email message.

Chat Room

An area on the Internet where two or more people can have a typed conversation in real time. In a chat room, the messages you type are shown instantly to every other member of the room. Messages typed by other people are shown immediately to you.

Computer Virus

A software program that attempts to affect your computer without your permission. Someone writes viruses for a specific purpose, usually to cause damage.

Cookies

A website's way of keeping track of you. It's a small program built into a web page you visit that can be left onto your computer. Typically you won't know when you are receiving cookies.

Download

To copy a file from a computer on the Internet to your own computer.

Email filter

Removes spam from your email inbox and places it in a separate folder, usually "junk mail."

Firewall

A program or system of protections to keep out unauthorized persons from accessing your computer.

Hacker

A person who breaks into a website or into an email box, usually to cause harm.

IP address

The "address" of a computer. Every computer has an IP address so that when we are online and upload/download information, other computers can find our computer and send us info.

Instant Messenger

A program that allows you to write to friends who are also currently on the Internet in real time. Messages are sent and received instantaneously. AOL, MSN, and Yahoo are frequently used.

Pop-up Ad

A pop-up is usually a small window on your screen that suddenly appears ("pops up") while you are on the surfing the Web.

Spam

Junk email or unwanted email

RESOURCES

Websites

Technofile article, "Basic rules for keeping your computer safe."
<http://aroundcny.com/technofile/texts/bit121299.html>

BBC article
<http://news.bbc.co.uk/2/hi/technology/2143630.stm>

The Federal Trade Commission
<http://www.ftc.gov/bcp/online/edcams/infosecurity/coninfo.html>

GetNetWise
<http://security.getnetwise.org/>

CERT Home Network Security Information.
http://www.cert.org/tech_tips/home_networks.html

Blue Kestrel Internet Security Tutorials
<http://www.bluekestrel.com/tutorials.htm>

Stay Safe Online
<http://www.staysafeonline.info/>

The Boomer Café article, "Getting Lucky With Online Dating"
http://www.boomercafe.com/Relationships/OnLine_Dating.htm

Anti-Virus Software

Norton Internet Security -- <http://www.symantec.com/product/>
AVG Anti-Virus -- http://www.grisoft.com/us/us_index.php
McAfee Virus Scan -- <http://download.mcafee.com/eval/evaluate2.asp>
VCatch -- <http://www.vcatch.com/>

Firewall Software

ZoneAlarm -- <http://www.zonelabs.com/store/content/home.jsp>
Kerio Personal Firewall -- http://www.kerio.com/kpf_home.html
Outpost Personal Firewall -- <http://www.agnitum.com/products/outpost/>
Sygate Personal Firewall -- http://smb.sygate.com/products/spf/spf_ov.htm

Top Internet Risks and How to be Safe

Remember – Our personal safety and our computer’s safety can be at risk when we use the Internet. Be a smart computer and Internet user and know how to protect yourself from fraud, personal danger, and computer damage.

| Risk | What you can do |
|---|--|
| Risk #1 Pop-up Ads | <ul style="list-style-type: none"> ① Learn to recognize ads on a website. ① Only click on those ads that seem like they might be helpful. ① Don't download anything until you have checked out the company ① Don't believe what ads tell you! |
| Risk #2 Cookies | <ul style="list-style-type: none"> ① Delete your cookies once a day or once a week! ① Disable cookies completely. |
| Risk #3 Online Shopping | <ul style="list-style-type: none"> ① Only deal with reliable online shopping sites ① Shop with companies that have an online privacy policy. ① Never buy anything from an unsolicited email or SPAM! |
| Risk #4, #5 and #6 Internet Dating, Chat Rooms, and Instant Messenger | <ul style="list-style-type: none"> ① Never reveal personal information until you are ready ① Stop communicating with someone if you feel uncomfortable ① Use an anonymous email address ① Talk on the phone first and use an unlisted phone number ① Always pick a public place to meet and let someone know where you will be. |
| Risk #7 Email Attachments | <ul style="list-style-type: none"> ① NEVER open an email attachment from someone you don't know. ① Delete any email that seems suspicious |
| Risk #8 and #9 Spam and Phishing | <ul style="list-style-type: none"> ① Use an email filter ① Use an unusual email address ① Don't list your email on the Internet. ① Don't buy something from a spam email. ① Use more than one email address ① Don't give out personal or financial information via email ① Ignore "personal" emails that address you as "Dear Client" |
| Risk #10 Computer disks | <ul style="list-style-type: none"> ① Always save your work in more than one place -- on disk and PC ① Use Anti-Virus Software and regularly update it ① If your computer is infected disconnect from the Internet right away ① Use your computer's security features |
| Risk #11 Passwords | <ul style="list-style-type: none"> ① Use passwords that are hard to guess ① Make your password easy to remember |

