



LINC Project * Welfare Law Center | 275 Seventh Ave #1506,
New York, NY | www.lincproject.org * 212-633-6967

Good Computer Usage Practices for Organization Members and Staff

Sometimes, it can seem almost impossible to keep a computer healthy, happy, and virus and spyware free. Computers have lots of vulnerabilities, and there are lots of people who try to take advantage of them. Keeping your computer safe can be an overwhelming task!

Don't panic. There are some easy things that you can do to help protect the computer you're using from viruses, spyware, and other things that can hurt it. They don't take any computer expertise – just some patience and care.

Tip #1: Don't Download, Don't Install!

One of the quickest ways to get viruses and spyware on your computer is to download things from the Internet. It's easy to make mistakes when downloading, because things that look like legitimate, harmless downloads are often viruses and spyware in disguise.

So – **don't download or install anything.** That includes music, instant messenger programs, file sharing programs, screen savers, desktop backgrounds or software. If you need something installed, talk to the person in charge of computers and technology at your organization first – they'll be able to make a good choice about whether what you want is needed and safe, and will be able to install it properly.

Tip #2: Beware of Pop-Up Scams

Viruses, adware and spyware are good at tricking us into thinking that we're downloading or installing things that are good for our computer. Lots of times when you're surfing the web, you'll get pop-up ads that say things like, "Your computer may have viruses – click here to protect your computer!" Sometimes these pop-ups look just like messages from Windows or another legitimate program. However, when you click, you wind up with something you don't want – perhaps a program that you don't really need, that's not really good, and that you have to pay for to get it to do the things it promises. Or, worse yet, you can get stuck with spyware or adware that ranges from the annoying to the downright destructive.

Ignore and close pop-up windows that claim something's wrong with your computer and that you need to "click here" to fix it. The computer you're working on already has all of the virus and spyware fighting software that it needs. Don't click "OK" – just close the window using the "X" button in the upper right hand corner.

One note: It's important to learn the difference between pop-up ads that are telling you that you have viruses or spyware, and notifications from the legitimate antivirus and anti-spyware software that organization's tech person has installed. Until you can tell the difference, the best thing to do is to ask someone in the office who understands computers better for help if something pops up on your screen and tells you there's a virus or spyware. But always ask first – don't just guess or trust what the message is telling you!

Tip #3: Be Smart and Safe About Emails

Another common computer vulnerability is email. Email can be used to try to scam people into handing over personal information. They can also come with attachments – files that are delivered along with an email – that include viruses. Here are some tips for figuring out which email messages are safe and legitimate, and which ones aren't.

Email Scams

- Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. **If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious – these are usually scams.**
- **Be especially suspicious if these emails are not personalized at all.** Usually, an email that's legitimate will include your name or username or something else about your account.
- If it's from a bank or company that you don't have an account with, you know it's fake, so just delete it.
- **If you're at all unsure or suspicious, don't reply or click on any links in an email to get to a web page.** If you're worried that an email is really from your bank or from a legitimate company, you can either call the company on the phone and ask them about it, or you can log into the company's website directly – don't click on the link, just type in the address of the website directly into your web browser and log in that way.

Email Attachments

- Antivirus software can be a big help when it comes to attachments, because it can scan an email attachment before you open it and warn you if there's a problem with it. **If the antivirus software on the computer warns you about an attachment, don't ignore the warning!** Instead, do not open the attachment, and delete the email and the attachment (or, if the antivirus software gives you the option of letting it delete it for you, let it delete it.) If the attachment was sent by someone you know, give them a call or email them directly and let them know that your antivirus warned you not to open it.
- **Never open attachments from strangers.** If you don't recognize the name or email address of the person who's sending you an attachment, don't open it – delete it.
- **Even if you know the sender, if you weren't expecting an attachment from them, don't open it.** Some viruses spread themselves by sending email that pretends to be from someone you know. If you think it's weird or unusual that someone is sending you an attachment, contact them first and make sure they sent it before opening it.

Tip #4: Use Firefox, not Internet Explorer

When you're surfing the web, you're using a program called a web browser. There are a few different web browsers out there, each with its own look and feel and features, but most of which work pretty much the same way.

Internet Explorer is the most common web browser, but it has many flaws and vulnerabilities that viruses and spyware take advantage of. Mozilla Firefox is another web browser. It's not as widely used, but it is recognized as being safer and more secure than Internet Explorer. It has less security flaws, and is also better at stopping pop-up ads.

So, when you need to use the web, use Firefox, don't use Internet Explorer.

GOOD:



This is the **Firefox** icon. Look for this on your desktop or in your Start menu and use it when you want to use the web.

BAD:



This is the **Internet Explorer** icon. If you have Firefox, use that – don't use this!

Other Resources

These websites were used as references when writing this primer, and provide more information on the topics covered here.

Safe Computing from the University of Chicago. Some of the things they mention are specific to the university, but this is also a very good general guide to safe computing. <http://safecomputing.uchicago.edu/practices/>

Consumer Advice: How to Avoid Phishing Scams from the Anti-Phishing Working Group. Good advice on how to protect yourself from email and web scams. http://www.antiphishing.org/consumer_recs.html

Published April 2006