
Feature

**Viruses 101**

*everything you need
to know about
computer viruses*

Inside

Viruses 101

*Everything you need
to know about viruses*

CyberEthics

*Being a good
CyberCitizen*

Mailing Lists

An Introduction

Hot Potatoes

A Tool for Teachers

Education's
Computing
Department

BuffaloState
State University of New York

 Buffalo State College

EDC NEWSLETTER

 Advancing Education through Technology

Volume 2, Issue 2

February 2004

FROM THE EDITOR...

Welcome to the February edition of the EDC Newsletter. As many of you know, the EDC Newsletter was created as a resource for EDC students, but has since grown to serve the general public as well. We count on our readers to provide valuable feedback and suggest new topics of interest. As your new Editor in Chief, I look forward to introducing you to new topics regarding educational technology.

This month's featured article focuses on computer viruses. As a network administrator at Erie Community College, I know the risks that computer viruses pose. While, some viruses are mere annoyances, others can be very dangerous. It is important to be educated about the different types of viruses and what you can do to protect yourself against them. In the article, we will cover the different types of viruses, explain how viruses spread, learn about antivirus software and give tips on protecting yourself from viruses.

I hope you enjoy this month's newsletter. If you have any suggestions, comments or corrections, don't hesitate to E-mail me.

Joseph Lundin

Joseph Lundin
EDC Newsletter Editor in Chief
lundjp88@mail.buffalostate.edu



Contents

Front Page

From the Editor

Viruses 101

All about Viruses

CyberEthics

Being a good CyberCitizen

Mailing Lists

An Introduction

Hot Potatoes

A Tool for Teachers

Mailing Lists Links

EDTech Discussion Network

Education Listservs

Educational Discussion Lists

Topica's Mailing Lists

Education
Computing
Department

BuffaloState
State University of New York

Buffalo State College
EDC NEWSLETTER
Advancing Education through Technology

Volume 2, Issue 2

February 2004

[Printer Friendly Page](#)

Mailing Lists: An Introduction

While browsing the Internet, you may have come across the term mailing list or Listserv™. If you are not already subscribed to a mailing list, you may be wondering what they are and if these lists could be helpful to you. Also, a commonly asked question is to explain difference between a mailing list and a Listserv™? This article should answer most of your questions, and get you started with mailing lists.

**“There a millions
of mailing lists
available on the
Internet”**

A mailing list is simply a method of sharing information via E-mail. There a millions of mailing lists available on the Internet, regarding almost any subject imaginable. Each mailing list has an E-mail address, just like you may have an E-mail address. However, when you send an E-mail to the mailing list address, it automatically distributes it to all the list subscribers, or members. If the mailing list allows it, the subscribers of the list are able to reply back to the list.

So a mailing list makes it easy for a large number of users to communicate via E-mail.

Those of you, who are E-mail experts, may be wondering if a mailing list is the same as a distribution list. While both are used to E-mail a large number of people, a mailing list has much more flexibility. For starters, people can choose to subscribe or unsubscribe from a mailing list, where as with a distribution list, the recipients cannot easily do this. Another difference is that with a mailing list, all you have to share is one E-mail address, not the entire distribution list. As you will see below, mailing lists have other features which are explained below.

To subscribe or sign-on to a mailing list, a user either sends an E-mail to the mailing list with a join command, or uses a Web Page to subscribe. Once you subscribe to the mailing list, you will start seeing the list messages in your E-mail. If you subscribed to a heavily utilized mailing list, you should be prepared to receive lots of E-mail. Most lists allow you to digest the message, which means instead of receiving separate E-mails for each post, you can have all the messages from that day or week come in one big E-mail. If you no longer wish to belong to the mailing list, you can always unsubscribe, which is done similarly to subscribing, except you use the unsubscribe command.

For those of you familiar with mailing lists, you may have heard the term Listserv™. A Listserv™ functions the same as a mailing list, but it uses different software. Listserv™ is a trademarked name, in order for a mailing list to be called a Listserv™, it must be running L-Soft international, Inc.'s Listserv™ software. Unfortunately, many people are not aware of this, and will mistakenly call their mailing list a Listserv™, even though it operates with a different mailing list application.



So, now that you know all about mailing lists, you may be wondering where you can find some decent educational ones. Some of you may even want to start your own mailing list, so you can easily communicate with co-workers, students or people who have the same interests. Look no further, the links on the left should help you get started with mailing lists.



Contents

Front Page

From the Editor

Viruses 101

All about Viruses

CyberEthics

Being a good CyberCitizen

Mailing Lists

An Introduction

Hot Potatoes

A Tool for Teachers

CyberEthics Links

CyberEthics for Kids

Resources for CyberEthics

Education's
Computing
Department

BuffaloState
State University of New York

Buffalo State College EDC NEWSLETTER

Advancing Education through Technology

Volume 2, Issue 2

February 2004

[Printer Friendly Page](#)

CyberEthics: Being a good CyberCitizen

**“We all need to
be responsible
while using the
Internet”**

The anonymity of the Internet has caused a lot of people to engage in unacceptable practices while online. However, it is important to realize that the Internet is not anarchy, where people can do anything without consequences. The Internet is a complex interconnection of billions of computers and people that spans many countries. While the Internet is not centrally governed, portions of it are covered by local and federal laws. Users of the Internet

need to act in a responsible manner while online, and those of us who are educators should remind their students of this.

So what are some general guidelines to follow while online? The most important are safety issues for younger children. You want to make sure children understand that they never to give out passwords, E-mail address, phone number, home address or any personal information on the Internet. This includes chatrooms, Instant Messages, Web sites or E-mail. Some issues that deal with children and adults include hacking, or breaking into another person's computer, stealing copyrighted material such as software, music, text or photographs from the Internet without permission and claiming publications written by someone else as your own.

Then there are the other CyberEthic issues that are not as obvious. It is unacceptable to send out unwanted E-mail to users, especially chain letters or advertisements, this is known as spamming. Users should be wary of scams or pyramid schemes, which can take many forms, such as eBay auctions and E-mails that promote get rich schemes. Forgery is a big problem on the Internet, including E-mail addresses, Web sites and identification theft. For instance you may get an E-mail that appears to be from a reputable company and directs you to an official looking Web page which asks you to verify your credit card information. The last issue is pornography, which is found almost every place on the Internet. Even innocent users could accidentally find themselves on pornographic sites if they do a single mistype, like typing in <http://www.whitehouse.gov> instead of <http://www.whitehouse.com>. While most schools may have filtering software, most homes do not. Proper precautions such as installing filtering software, or parental supervision while browsing should be practiced.



We all need to be responsible while using the Internet. The Internet is an enormous resource of information for adults and children. Users should be aware however, that the Internet is much like a city. There are some places that are safe and wonderful, and others that you should avoid.



Contents

Front Page
From the Editor

Viruses 101
All about Viruses

CyberEthics
Being a good CyberCitizen

Mailing Lists
An Introduction

Hot Potatoes
A Tool for Teachers

Viruses 101 Links

Symantec Security
Response

Mcafee Virus Info

Trend Micro

AVG Free Edition

ZoneAlarm Free Edition

Microsoft Windows XP

Education
Computing
Department

Buffalo State College
EDC NEWSLETTER
Advancing Education through Technology

Volume 2, Issue 2

February 2004

[Printer Friendly Page](#)

VIRUSES 101

The History of Computer Viruses

Before the Internet became popular, computer viruses were localized and did not infect millions of computers. Most of these computer viruses were spread by floppy disk and were simple to detect. Antivirus scanners were so small that you could fit them on a single floppy disk, and most home users did not even own an antivirus scanner. After the popularity of the Internet, came the explosion of computer viruses. Viruses such as W97M.Melissa and

VBS.Loveletter suddenly started spreading to millions of computers. These new viruses not only spread faster, but also caused devastated effects. Take for instance, the VBS.Loveletter virus, which overwrote files that ended with .DOC, .JPG, .GIF, .MP3 and others with the actual virus. As these viruses became more widespread, the public

turned to antivirus companies such as McAfee, Symantec and Trend for protection. Antivirus software became common on home computers, especially those who used the Internet. Today, almost every computer user has heard of a computer virus and most likely even experienced one firsthand. The viruses of today, can spread faster and are harder to detect. Recent viruses such as the CodeRed Worm, W32.Blaster and W32.MyDoom virus infected billions of computers and costed companies millions to clean up.

"After the popularity of the Internet, came the explosion of computer viruses"

What is a Computer Virus?

A computer virus is a small computer application. For example, when you double click on the Microsoft Word icon, you are executing programming code to open Microsoft Word, which is a computer application. A virus is very similar, but it is a much smaller application, and when you execute it, the virus runs malicious programming code. So where does this programming code come from? Basically, almost anyone knowledgeable of programming can write a virus. Some viruses were written by kids, others by adults and these viruses can be distributed from anywhere in the world, thanks to the Internet. To make matters worse, there are even easy to use virus creation programs, that lets anyone create a virus by a few simple mouse clicks.

There are many different categories of computer viruses. Two of the more common types of viruses are worms and trojan horses. A worm is a virus which has the capability to spread itself over the network or Internet. Sometimes the worm will replicate itself by sending out mass E-mail from the infected computer, other times it may take advantage of security vulnerability in an operating system. For example, the W32.Blaster worm infected computers using a known vulnerability in the Windows operating system. A trojan horse is a virus program which after infecting a computer, will create a backdoor into that computer. This backdoor will allow other users to gain access to the computer to steal information such as passwords or credit card numbers and allow them full control over the computer. If a user gains control of your computer, they can use it to hack into another computer, or launch virus attacks from it.

How to Protect Yourself

It is now more critical then ever to protect yourself from computer viruses. There are many steps you can take to protect your computer from being infected. One of the most





important step is to install antivirus software on your computer. Antivirus software works by keeping a large database of virus identifying characteristics, known as fingerprints. The software constantly scans files that are opened on your computer, looking for a fingerprint. If it recognizes a virus the antivirus software will deny access to it and either attempt to repair the file, or quarantine it. Since the antivirus program will only recognize viruses that exist in its database, you must keep it updated. This is why it is necessary to download new virus definitions, so your antivirus scanner can recognize newer viruses. Some newer antivirus programs also use heuristics to detect viruses, which look for virus-like activity in programs, instead of fingerprints. There are many virus scanners available today, some cost money such as Symantec AntiVirus and McAfee VirusScan, others free scanners like AVG Anti-Virus Free Edition.

If you are a Microsoft Windows user, it is important to keep your operating system patched. Patching your operating system fixes security vulnerabilities that may be used by viruses to compromise your system. Users should visit the Windows Update site at <http://windowsupdate.microsoft.com> to make sure all the critical patches have been loaded.

Personal Firewall software, such as Zone Labs' ZoneAlarm can also provide protection, by blocking vulnerable TCP/IP ports on your computer. TCP/IP ports are open connections to the Internet which are addressed based on the service they provide. For example, port 80 is the TCP/IP port for HTTP or Web traffic. By using a firewall to protect incoming and outgoing ports, you can reduce the likelihood of an infection. For example, if a virus is spreading via TCP/IP port 135 (like the W32.Blaster worm used) and that port is blocked with firewall software, your computer will not be infected. For those using Windows XP, there is a basic built-in firewall included for free. For more information on how to enable the firewall, go to your Start Menu, Help and search for firewall.

Finally, the most basic protection is common sense. When using E-mail, never open unexpected attachments, even if you know the person. Newer E-mail viruses will forge the from address with a random address found on the infected computer. Thus, the sender may be someone you know, but if you were not expecting an attachment from that person do not open it. Also, be cautious when downloading files from the Internet, only download from reputable sites. If you use Peer to Peer software such as Kazaa, iMesh or eMule (to share legal multimedia files) be sure to use an antivirus scanner and do not download suspicious files.

Now that you have a basic understanding of viruses and how to protect yourself, take the steps necessary to secure your computer. Viruses can be very damaging, and they will continue to spread if people do not protect their computers.



Contents

Front Page
From the Editor

Viruses 101
All about Viruses

CyberEthics
Being a good CyberCitizen

Mailing Lists
An Introduction

Hot Potatoes
A Tool for Teachers

Hot Potatoes Links

Half-Baked Software

Hot Potatoes Hosting
Services

Education's
Computing
Department

BuffaloState
State University of New York

Buffalo State College
EDC NEWSLETTER
Advancing Education through Technology

Volume 2, Issue 2

February 2004

[Printer Friendly Page](#)

Hot Potatoes: A Tool for Teachers

Hot Potatoes, created by Half-Baked Software Inc., is a software application that creates interactive Web-based teaching exercises. The software is normally \$100 per copy, but is free for educational and non-profit institutions that make the material available for free on the Internet. The software has six different components, JCloze, JMatch, JQuiz, JCross, JMix and The Masher. The JCloze component creates a fill in the blank exercise, where teachers can provide clues to help their students type in the correct word to complete the sentence. JMatch builds a Web application, where students need to match words on the left, with jumbled up words on the right. JQuiz is a Web-based quiz, which allows teachers to use four different question types, including multiple choice and short answer. The JCross component builds crossword puzzles that can be completed on the Web. JMix creates jumbled-sentence exercises allowing students to put the sentence in the correct order. Finally, The Masher component will put all your Hot Potatoes exercises into one large Web site, so students can easily navigate through them.



I found the Hot Potatoes software to be easy to use. The software uses .HTML and JavaScript, which is compatible across most browsers. One of the problems with Hot Potatoes is that you can not log the student's activity through the exercises. If you are interested in tracking students and grading them on Hot Potatoes activities, you can check out <http://www.hotpotatoes.net>. Hotpotatoes.net, for a fee, will host your Hot Potatoes activities, and track students' usage. Prices start out at \$90.65 for one year of hosting, up to 50 students and 10MB of space.

Hot Potatoes version 6 is currently available for all Windows operating systems. Unfortunately, while there is an older 5.3 version of Hot Potatoes for the Macintosh, there is no version 6 yet. For more information, or to download the software, visit <http://www.halfbakedsoftware.com>

[Click Here for a Sample Test created in Hot Potatoes](#)