

E-mail Safety Guidelines

Statistically, more viruses are spread by e-mail than any other means. Here are a few steps to help protect you when using e-mail.

1. Prescreen your messages

Examine your list of unopened messages carefully before you open any of them. If you didn't expect a message, if you don't know the sender, if the subject or attachment seem strange, too urgent, too alarming, too good to be true, or the sender and the subject don't jive, just delete the message, along with any attachments, without opening it.

2. Don't click that link

It's very easy to "spoof" links in e-mail messages so that they look like they're legitimate, but they actually take you to a counterfeit or hostile Web site. Treat links contained within e-mail messages as suspicious.

3. Weed out obviously bogus messages and attachments first

You need to examine messages and attachments as a whole, not separately. Sometimes attachment details -- size, name or extension -- combined with the nature of the message will tell you they're bogus. Usually there's a sense of something not quite right. If something is fishy just delete the message, along with the attachment - when in doubt throw it out.

HTML attachments (filename.htm or filename.html) are a special case. Depending on how the message is composed, and on its size, e-mail clients will show some HTML messages as attachments. Others will be displayed directly with no attachment. Either one can have malicious content though.

Many malicious attachments appear to come from a legitimate address, or from someone you know. Be suspicious of any attachment that you were not expecting -- even though it's from someone you know. Be paranoid about attachments from anyone you don't know.

4. Ignore the SPAM

Don't reply to unsolicited messages ("spam") mail, or other harassing or offensive mail. By responding, you only confirm that you are a person with an active e-mail address who can be plagued with constant unwanted e-mail solicitations. Instead, forward the unsolicited message to the customer service department of the source's e-mail (usually of a form similar to [abuse@\[implicateddomain\].com](mailto:abuse@[implicateddomain].com)). To help control spam, Buffalo Trail uses SPAM filter technologies, but blocking SPAM is a delicate art - block too much and legitimate e-mail messages go missing; not enough blocking and our systems get filled with "junk" messages.

5. Beware of Phishers

Brand spoofing or phishing is a scam where the perpetrator sends out legitimate-looking e-mails appearing to come from a legitimate company in an effort to phish (pronounced "fish") for personal and financial information from the e-mail recipient.

Be wary of e-mails with links to web sites, coming from parties pretending to be legitimate companies, requesting personal or financial information. If you receive one of these e-mails, delete it immediately and do not respond or act on it.

Always remember, legitimate companies will never send customers an e-mail asking for passwords, account numbers or personal information.

6. Handle attachments with suspicion

A good rule to follow is - *DO NOT open an e-mail or attachment that you are not expecting.*

Viruses often come disguised as e-mail attachments (sometimes signified with a paper clip), with a subject or file attachment name that entices you to view it. As soon as you view the e-mail or open the attachment, the virus is unleashed into your computer. If you receive an e-mail from someone who you're not expecting an attachment from or with an odd subject, call the person first to see if they knowingly sent you the e-mail.

When you send an e-mail with attachment, it is very helpful to the person receiving the e-mail if you give a very specific subject so that they know the e-mail is legitimately from you. A subject line of "Attached School Budget 2004-2005" is an example of a good, very specific subject line.

Never, ever open an e-mail attachment that you have any doubts about -- even if it's addressed directly to you and comes from someone you know. Always check with the sender directly -- most worms appear to come from someone YOU KNOW. When in doubt verify -- make sure they intended to send the attachment. (Just send them an e-mail and ask what it's all about)

If it has a filename with a double extension, like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that to find out whether it's a program masquerading as a data file, such as a text file or jpeg (graphics) file.

If an attachment has one of the following extensions - .bat .exe .vbs .pif - be very careful!! Files of this type are executable - this means that they are programs that can run on your computer and they should be considered very suspicious.

If an attachment has one of the following extensions - .rtf .xls .doc .ppt - these are common file types used by Microsoft Office. They can contain macro viruses but are usually safe.

If an attachment has the following extension - .pdf - this is an Adobe Acrobat file. PDF files can generally be trusted to be safe: there are no major/common viruses that infect .pdf files.

If an attachment has one of the following extensions - .gif .jpg .bmp .tiff - these are common graphic image (picture) files. These files can contain viruses, but are not commonly targeted by viruses.

If an attachment has the following extension - .zip .cab .tar .rar .lzh .lha .bz2 .arj - these are common compressed (zipped) file types. ZIP files are often used as e-mail attachments because they compress the original file making it smaller and easier to send. The problem is that ZIP files are also commonly used by viruses. ZIP files are very useful and in common use - use them with caution!

It all comes back to "the good rule" - DO NOT open an e-mail or attachment that you are not expecting!

7. Common Sense

Use common sense when you're on the Internet and maintain a healthy dose of skepticism. Use caution when revealing personal information, such as your physical address, to anyone you meet in cyberspace, even if they claim to be someone of authority.

SAFE E-MAIL PRACTICES FAQ (Frequently Asked Questions)

Q1: Why is it important to practice safety in reading E-mails?

There has been a high increase of malicious codes such as virus, worms and trojans that spread via E-mail attachments, notably due to the lack of caution and care by individual in handling E-mails. On the other hand, viruses can spread via diskette and file downloads too, however, the impact has not been as widespread as via E-mail attachment.

Q2: How fast can these virus spread?

The speed at which these malicious codes spread depends on the behavior of the virus itself, notably the worm type viruses spreads automatically via E-mail attachment, which the code itself initiates. The user will not be aware that a mail has been sent from his/her PC to his/her friend. This Worm feature can create payload on the user's or the service provider's mailer system, e.g., Happy99* (<http://www.mycert.mimos.my/virus-info/happy99.html>) and Melissa Worm* (http://www.cert.org/ftp/cert_advisories/CA-99-04-Melissa-Macro-Virus.txt).

Q3: What damages can these malicious codes do?

Malicious codes that have features to destroy data, such as Worm.ExploreZip* (http://www.cert.org/ftp/cert_advisories/CA-99-06-explorezip.txt) and CIH* (<http://mycert.mimos.my/>) will destroy files, harddisk partitions, bios and other possible damages to the systems and hardware. Malicious codes with trojan features, on the other hand, will open a backdoor on the victims' machines inviting remote entry to the system.

Q4: How advanced is the threat?

The threat has been increasing since mid 1998. We've see many recent malicious codes that have combined features of virus, worm and trojan, which increases the threats and challenges to the IT industry, especially to the antivirus vendors in coming up with fixes. Our observation is that the most active attacks since mid last year have been on the Windows platform. The statistics of reports received by MyCERT are available at <http://www.mycert.mimos.my>.

Q5: How do we prevent the spread of these malicious codes?

Practice caution when receiving E-mail attachments. Upon receiving E-mail with an attachment, use extreme caution.

- **DO NOT CLICK THE ATTACHMENT**. Do not open it, do not view it, and do not save it to disk.
- Verify the E-mail, by contacting the sender.
- Do not launch the program automatically - save it to hardisk to enable the antivirus software to scan the file for any viruses.
- Ensure you have your antivirus, virus list updated.
- If your computer shows some sign of abnormalities, after you launch the E-mail attachment, contact the sender.
- Contact your Network Administrator if you are at your office. If you are at home, contact your ISP (Internet Service Provider). **DO NOT SEND THEM A COPY OF THE ATTACHMENT**, describe it to them and then wait until they ask you for it.

Upon sending out an attachment, practice the following:

- When sending an attachment, write the message describing the file and why you are sending it. Remember, viruses can do this too, so try and include something unique in this message so the recipient will know it is from you and not some automated virus.

Q7: What if the E-mail is an announcement from my ISP, which includes an attachment?

ISPs will **NOT** send documents attached to an E-mail announcement. They would normally refer to their webpage, where you can retrieve the desired information.

Don't open e-mail attachments that have file extensions of .bat, .vbs, .shs, .pif, or .scn if you can help it—Safe attachments rarely use these extensions, but they're a favorite choice among virus writers because they can carry executable instructions.

Some Basic Guidelines

Handle Attachments Safely.

- Don't open attachments unless you are absolutely sure about what they are and who they came from.
- Even attachments that were sent directly to you by a known sender might contain malicious code. Many viruses *Spoof* the sender's address – just because the e-mail says it is from admin@btps.ca, it may be from nastyvirus@spoofer.hacker.net - **this is why descriptive subject lines are important.**
- Be especially careful with MS Word & Excel files.
- When opening unknown or untrusted Microsoft Word or Excel attachments containing macros, always select the "Disable Macros" option.
- **Beware of Dangerous File Types! - .bat .exe .scr .pif .vbs**
- Some malicious attachments will "pose" as a harmless file type like digital image by including that file type extension in its name. You might get an attachment called "hawaii.jpg" and think it's a picture from your friend's vacation. But it might actually be a .pif file, one of the exploitable file types. This can happen because Windows does not display file extensions by default, so a .pif file named "hawaii.jpg.pif" will appear as "hawaii.jpg" - **this is why descriptive subject lines are important**

Don't Unsubscribe.

Spammers often include an "unsubscribe from this list" link in their messages that makes them appear more responsible and reputable. This is a way to confirm your e-mail address so they can send you more spam or sell your e-mail address to other spammers. If you don't want it, mark it as junk and delete it.

Be a Good Internet Citizen.

- Don't use your e-mail in ways that will contribute to the problem.
- Don't send unsolicited e-mail and attachments.
- Don't forward chain letters.
- Don't respond to or participate in e-mail hoaxes.
- Don't send attachments which use the "unsafe" file types.
- Don't post your BTPS e-mail address (or other student's addresses) on publicly accessible web pages.
- Use a "disposable" e-mail account (a free account from yahoo or hotmail) for online shopping and posting to non-BTPS online discussion boards.