



**Subject: Children Online Newsletter**

You're receiving this email because you signed up at ChildrenOnline.org.

You may [unsubscribe](#) if you no longer wish to receive our emails.



Quick Links

- [Register Now](#)
- [Resources for Parents](#)
- [Children Online Website](#)

Join Our List

[Join Our Mailing List!](#)

**Protect Your Computer**

Without exception, all computers should have several layers of protection. These include:

1. Anti-virus software
2. Anti-spyware software
3. Firewall (software and/or hardware)

**Issue: #25**

**June 2009**

**25th Edition of the Children Online Newsletter.**

During the past few months there has been a significant increase in malicious emails sent as spam and flooding users in-boxes across the Internet. Children and teens, as well as adults, are easily fooled into clicking links or downloading files that may result in the installation of spyware or malware. And Apple's Mac users are no longer exempt from these threats. Mac owners may want to visit the [Sophos.com blog](#) to learn about two new threats discovered against the Mac OS. Though there are far fewer threats against the Mac operating system, these threats are on the rise.



Spyware is software that is installed on a computer, without the user's knowledge or consent, and searches for information valuable to the person who installed it. Such information

versions)

4. Strong passwords of at least 8 characters
5. Email accounts that offer anti-spam filtering services

Several reputable companies making quality products include [Symantec](#) (who also owns Norton), [Sophos](#), [Intego](#) (for Mac)

For additional information about several free anti-spyware products for PCs such as Ad-Aware and Windows Defender, visit [ChildrenOnline.org](#) and click on Resources. Next click "Protecting Privacy/Safety Online."

**RELATED TOPIC ARTICLES:**

1. [Windows Secrets article "Has your PC become a spammer's botnet zombie?" by Scott Dunn, January 2009.](#)
2. For those who would like to learn more about botnets, [WatchGuard.com produces a 3-part video series.](#)
3. Read Sophos'

could be used for direct financial gain, such as capturing bank or credit card login information, or for identity theft as well as other things. Spyware might include a key logger that captures every keystroke made on a computer and sends it to the person who installed it. Malware (bad software) is typically software that enables the installer to become a "superuser" with complete control over the computer. Such computers are called "zombies" and are remote-controlled by spammers to send out hundreds, or even thousands, of spam email per hour or conduct attacks against Internet web sites. Networks made up of hundreds or thousands of zombie computers are called "Botnets." A botnet "herder" may actually rent out there botnets on an hourly or daily basis in black markets across the Internet. Malware attacks have successfully turned millions of PCs into zombie computers and, until recently, this threat did not exist against Mac users. That changed last winter when the first Mac botnet was discovered. (The Macs became infected when users downloaded pirated software from "warez" sites that had been seeded with infected stolen software. [Read article.](#))

Unless your computer has multiple quality layers of protection (see resources in the sidebar), it is susceptible to these types of attacks. Our email boxes are being flooded with these attacks disguised to look like official emails from UPS, FedEx, state and federal government agencies, news organizations, and online services from trusted websites. It becomes very difficult to determine legitimate emails from malicious ones. This newsletter is meant to help children and adults tell the difference and learn "best practices" for using email more safely.

As always, we welcome your comments. Our telephone number for Children Online is 413-214-1225.

Wishing all of our readers a wonderfully relaxing and safe summer,  
Marje Monroe and Doug Fodeman

Contact Marje or Doug via email at [marjem@childrenonline.org](mailto:marjem@childrenonline.org) or [dougf@childrenonline.org](mailto:dougf@childrenonline.org) for information about our programs or consulting services.

blog post "[Celebrity News Still an Active Lure for Malware](#)"

**SAMPLE EMAIL HEADLINES THAT HAVE RECENTLY LINKED TO MALWARE:**

- Bred Pitt marks a birthday!!!
- Britney Spirs made a match!!!
- CIA tortures prisoners!!!
- Harry Potter was purchased by pentkhaus!!!
- Hillari Clinton stood up for daughter!!!
- Hollywood stars - George Clooney!!!
- Madonna reinvents herself as film director!!!
- Michael Jakson glued up a person a plaster!!!
- Mobile replacement of Blu-ray and HD DVD is created!!!
- Pamela Anderson divorces in third times!!!
- Princess Diana 'could have been killed by MI6' - conclusions of experts!!!
- Secrets of Cambridge 'porn' library revealed!!!
- The extramarital son of John Kennedy

## Teaching Our Children (and Ourselves) How to Determine Friend From Foe in Our Email In-Boxes

In my role as a teacher of educational technology, I am routinely reminding my faculty of the many threats and risks that are a mouse-click away. They, in turn, are usually very savvy and cautious. I knew that I had a problem, however, when a string of malicious emails with dangerous attachments recently passed through two layers of protection at my school and arrived into eight email in-boxes. Three of those eight people were tricked into double-clicking the attached files. Fortunately, a third layer of protection had stripped the attached zip file from the email and replaced it with a harmless ".txt" text message. (A zip file is a compressed file containing one or more files and who's content is masked until it is opened.)

Each of these emails looked as though they came from UPS.com with a subject line reading "Delivery problem" and containing a variation of the following message:

Dear customer!  
We failed to to deliver the package sent on the 13th of April in time because the recipient's address is incorrect. Please print out the invoice copy attached and collect the package at our office.  
Your United Parcel Service of America

Would you have fallen for this? These disguised attacks have been reported in the news online: [PCNews](#), [Sophos](#).

A similar ruse occurred at the end of May with emails purportedly sent from Western Union that read:

Dear customer!  
The money transfer you have sent on the 2nd of March wasn't collected by the recipient.

According to the Western Union regulation the transfers which are not collected in 15 days are to be returned to sender.

To collect money you need to print the invoice attached to this e-mail and visit the nearest Western Union

appeared in  
Canada!!!

- The first roller is  
presented to the film  
"Indiana Jons - 4"!!!  
- Two powerful  
earthquakes  
happened in the  
USA!!!

### RELATED FACTS FROM SOPHOS.COM

1. 90% of all spam originates from a botnet.
2. Well over 97% of business email is spam served up by automated software via botnets.
3. 1.3% of all Google search returns contain links to infected websites including popular sites; malware manufactures try to infect popular web sites for high visitor traffic e.g. USA Today, WalMart, Target and Unicef have all been recently exploited.
4. 85% of malware infected web pages are on legitimate web sites.
5. Newly infected hacked web pages are discovered by Sophos.com every 5 seconds.
6. IM and Skype have both been used as a tool to

agency.  
Thank you!

The expanding zip files attached to these emails install Trojan software giving complete control of your personal computer to the scammers who sent you the email. The folks that send emails of this type are often brilliant social engineers. One of their greatest talents is manipulating the behavior of the recipient. They must first get your attention with a subject line that will entice you to open the email. There have been thousands of effective subject lines including the recent lines listed below. Ask yourself if you or your children would have opened email because of these subject lines.

Order #42396	From your Insurance Commissioner
You're just so stupid	Your comment erased
Your request denied	Error in processing
Re: your order	Photos from weekend
Books you need	Free preview downloadable
Join our club	Mistake in your file
Answers for exams	Avril's nudity
Why don't you mail me	Re: Your order #349284
Someone replied to your comment	
Your profile doesn't answer	
Your email exceeded the storage limit	

Once opened, the scammer must next trick you into doing one of two things:

1. Click a link
2. Double-click an attached file

Younger children and teens are especially at risk. Younger children have little or no understanding of the disguised threats that pour into email accounts. Teens are exactly those who are most likely to click links disguised as notifications from Facebook, Twitter, MySpace, porn sites, or purported to be funny or embarrassing videos about celebrities. To greatly reduce your risk, and your children's risk for being the successful target of these email attacks, follow these guidelines.

**1. Don't click email attachments AT ALL unless you are expecting one or receive one from a highly trusted source.** If you receive an attached file that is suspicious, try contacting the sender to see if it is legitimately sent. Malicious

disseminate malware but the most popular method today is via infected web sites. 7. \$500 or more will enable a buyer to purchase malware kits which can be deployed to victims via email or an infected web site. The "drive-by" attack, whereby someone is tricked into visiting an infected web page, is the classic method for getting malicious software onto a person's computer.

### About Children Online

Children Online offers innovative and comprehensive workshops on Internet safety and online education to students, parents, faculty and administrators. Our approach, unique in the field of Internet safety, combines a thorough understanding of Internet technologies, child development and counseling, to focus on the impact of the internet on the social, emotional and language development of

code has been hidden inside photos (jpg files), pdf files, mp3 files (music files), Word documents (.doc/.docx), Excel documents (.xls/.xlsx) and even Powerpoint presentations (.ppt/.pptx)

**2. Don't click links embedded in emails, ESPECIALLY** those that say they lead to pornography, embarrassing images or videos, gossip about celebrities, or for images and sound files that say they things like "If you cannot see this image, click here." Here are a few recent examples from malicious emails:

- a. Angelina Jolie Nude. Click below to see.
- b. Paris Hilton Video. Information and links about the public scandal around Paris Hilton's alleged sex tape.
- c. Cameron Diaz naked? Yes sir. Click now to see!
- d. Christina Aguilera is a complete slut! She loves to get naked and have sex with just about anyone.
- e. Enimen buttface episode.

**3. Never open emails that look like they come from yourself** (unless of course you sent them.) It is a very common tactic for scammers to send emails to users that are spoofed to look at though the user sent it to him/herself.

**4. Never open emails when the user's name does not match the name that precedes the "@" in the address,** e.g. Legitimate: Doug Fodeman dfodeman@brookwood.edu NOT legitimate: Katharine <etxco@wii3.com>

**5. Unless you have good reason to expect communication from Russia or China, simply delete any email that appears to originate there.** Both Russia and China are one of the largest sources of spam and spyware/malware threats, next to the United States. Email that is sent from these countries, and not spoofed to look like it comes from somewhere else, will end with a recognizable country code. Their country code suffixes are:

Russia ".ru" e.g. "Lorie Larson<autonomousskkx@stelagi.ru>  
China ".cn" e.g. "Rocco Tabor" dredge0@skyon.com.cn  
Note: Country codes are sometimes misleading such as ".de" which is for Germany (Deutschland) not Denmark, or ".es" for Spain (Españ±a)

**6. If you do click a link you think you can trust and then find yourself being told that you need to install or download something in order to continue, DON'T!** NEVER click OK or Yes to download and install software to play a video, flash (animation) or sound file. Contact the website owner or originator of the email to ask if the request

young people.

Doug Fodeman and Marje Monroe, experts in technology, counseling and education, work together to provide invaluable research and tools for parents and schools with practical real-life solutions to the issues faced by young people online. Since 1997, Marje and Doug have spoken to thousands of students, teachers and parents. They have several publications in the area of Internet safety and offer a free online newsletter. More detailed information can be found at [ChildrenOnline.org](http://ChildrenOnline.org).



to install or download is legitimate.

**7. If it seems too good to be true, it is!**

**8. Just because an email's subject line says something about "your order", or delivery etc, doesn't mean it is legitimate.** An email recipient will naturally be curious enough to open an email if they are told it is something about their "order." However, if you've not ordered anything, be suspicious! Look carefully at the sender's address before deciding to open the email or not.

**9. Never open emails containing your email address in the subject line** e.g. To: Dougf@childrenonline.org

**10. Never click links in emails that are for eCards (online cards), online photo services, etc. in which the email contains no personal information identifying who they are from or originating from someone (full name) whom you do not recognize.** For example, this recently came from Snapfish, an online photo service. The recipient had no idea who the sender was.

Hi, Here are the photos of now and then.  
Enjoy  
Jan

Just today, the 15th, some of our users received phony eCards with links leading to malware.

Unfortunately a small group of unscrupulous people make our Internet experiences risky. We must constantly be on our guard. That is what we should be teaching our children as they grow up using the Internet. It is another reason why younger children are not developmentally prepared for the risks that can arrive in a user's in-box. Children Online does not recommend that children below sixth grade have their own personal and private email accounts. And all children and teens with email accounts need to be educated about the threats they may find in their in-boxes.

Â© Children Online 2009  
Doug Fodeman & Marje Monroe.  
For permission to reprint please contact  
[DougF@ChildrenOnline.org](mailto:DougF@ChildrenOnline.org)

[Forward email](#)

✉ **SafeUnsubscribe®**

This email was sent to dfodeman@brookwood.edu by [dfodeman@brookwood.edu](mailto:dfodeman@brookwood.edu).  
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



ChildrenOnline.org | 19 Everett Paine Blvd. | Marblehead | MA | 01945