

To: All CUSD Employees
From: Ray Quinto, Information Services Supervisor
Re: Unwanted emails messages (spam)

Greetings,

There have been a recent increase of unwanted email messages which is causing some concern amongst our user community. The request I have been getting most often is "please stop them." In an effort to explain what is happening and the realities of the internet, I've come up with this message and placed it on the website in hopes I don't have to respond to every phone call or email that gets forwarded to me with the same message. Let me try to answer some of your questions in the following Q&A format:

1. Why do I get these unwanted and sometimes offensive messages?
 - a. The internet was created to propagate messages. It does a real good job getting you the messages that are addressed to you or a group list to which you subscribe.
2. How did a "spammer" get my email address? I never sign up for anything on the internet.
 - a. Once you send an email, the recipient has the option to put your email address in their address book. If your address is in someone's address book and their machine is compromised by a virus, then your email address is compromised.
3. What's a virus?
 - a. A "computer" virus is a software program that an evil person created to make life difficult for you and me. Viruses come in many varieties and the majority of them are designed to steal information from your computer and turn it around to annoy the rest of us. The way the program works is once it is allowed to run on your computer it goes looking through all your files and finds any instance of an email address, or credit card number or other interesting information the evil person wanted to retrieve. Many programs then sit dormant in your machine and at a predetermined time, wakes up and becomes a mass e-mailing machine using every address it can find on the infected machine. The more computers that get infected, the more junk emails we all get.
4. Why did I get a spam email from an email address from someone I don't know?
 - a. See question #3. Once a machine has been infected and the dormant program wakes up to do the mass e-mailing it uses every email address it can find to send the email. So if your email address book has 10 unique addresses in it, the evil program will send out 90 spam messages. E.g., evil program using address1@domainX.com will send to address2@domainY.com, address3@domainZ.com, address4@domainAA.com, and all the way down to address10@blah.blah

for a total of 9 messages. Since a computer is really good at doing repetitive functions, guess what? The evil program then uses address2@domainX.com and sends a message to address1, address3, address4, etc. It continues to do this until it cycles through all 10 addresses for a total of 90 messages if my math is correct.

5. Why do I keep getting spam over and over? Is my address in that many infected machine address books?
 - a. See question #3 and #4. Some evil virus programs are designed with a “variable payload.” Geek speak for: the evil program can change what it sends out in the subject: line and what’s in the message body. The really clever ones (booo!) can vary the variables by substituting junk characters in the message or change the text by inserting spaces or other legal characters (apostrophes, tilde, etc.). In this scenario, a single machine with a clever and evil program running can send out thousands of annoying email messages per hour if it has enough email addresses to work with.
6. I hear you have spam filtering on our network. Why aren’t you blocking the annoying messages?
 - a. Spam filtering software was developed to fight the clever and evil spam we all want to see go away. The software runs on computers which I mentioned in #4 is really good at doing repetitive functions. Along these lines, spam filtering software only works if it can make a positive match on what it needs to filter. If the match happens, the filter whacks the message and you never get it. Spam filters cannot “guess” and make a determination like you and I can. It has to be a 100% match before it can act on the email. Anything less will allow the email message to pass through. Do you ever wonder why there are spaces or weird characters in the subject line or body of the spam you get? Variations in the characters are intended to fool the spam filtering software.
7. I’m always getting the same obnoxious email over and over. It comes from different source addresses and the subject line is different each time but the body of the message is always the same offensive stuff. How come you haven’t whacked this message yet?
 - a. The evil spammers have figured out that embedding a picture file(s) in the body of the email with the text or graphic in the picture file gets around the spam filters. The spam filters are looking for a text string. The text is part of the picture file so there is no text to filter on. The only option here is to disallow all emails with picture files. This would kill off all legitimate emails with attached pictures. The really clever and evil spammers create a picture with a white background making the text in the picture appear as though it is normal text. Most of us use a white background with black letters as our default so the message appears as though it is plain text when it is really a picture.

8. The spam filter is working but I still get junk messages. What's up?
 - a. The spam filter software is installed on a computer at the edge of our network. This is to protect us from the ugly stuff coming in from the outside world. Picture this: a bicycle wheel. Your worksite is at the end of one of the spokes and the spoke is connected to the hub (district office). CUSD has many sites (spokes) and the district office is connected to another larger wheel at Butte County Office of Education (the edge of our network). BCOE is our internet service provider. If you have a connection at home, your internet service provider may be SBC (now AT&T), AOL, Earthlink, Outrageous, or bunch of other possible vendors. Within our own bicycle wheel (aka domain), all of our sites are connected but email messages between us do not go out to the edge where the spam filter is located. If one of our machines get infected then the evil email program can mass mail the rest of us without any resistance. The IT department is working on installing anti spam software on our mail servers. One server is being scanned for spam and we will have a solution for the second mail server in March of 2006.

As you can see, the battle against spam is challenging. Our technology is constantly being surpassed by clever people with lots of money and time to figure out how to deliver junk to you and me. As many of you have experienced, a perfectly normal looking email in our inbox when opened displays an offensive picture. We can never guarantee 100% filtered and clean emails but the IT department in partnership with BCOE will be vigilant at keeping our systems updated with the latest tools and techniques at stamping out unwanted email messages. Over the last 12 months, our effectiveness at reducing unwanted junk emails has been very high. High, but unfortunately not perfect. Thank you for your patience and understanding as we wrestle with this industry wide problem.

Ray

For further reading please see these links:

<http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12>
<http://www.washingtonpost.com/wp-dyn/technology/specials/spam/>
<http://www.pcworld.com/news/article/0,aid,116300,tfg,tfg,00.asp>
<http://www.sciam.com/article.cfm?chanID=sa006&articleID=000F3A4B-BF70-1238-BF7083414B7FFE9F&pageNumber=1&catID=2>

A simple search on your favorite search engine will yield loads of other reading material.