

Some General Information Regarding Spam

Xenia Community Schools IT Department

What is Spam?

Spam is an unsolicited e-mail you receive. It's usually commercial advertising and is frequently for dubious products, get-rich-quick schemes, or illegal services.

The first step in combating the onslaught of spam is to know it when you see it. If you're lucky, you can identify spam based on its subject line. If it's offering you a lower mortgage, a date with Trixie, or free \$\$\$, you know it's spam. But be careful, because spammers often use guile to make the subject line something you might click on, such as "FWD: great punch line." So, even if the subject looks harmless, your best bet is to just delete it if you don't recognize the address.

Many spammers also fake the name of the sender with something common such as "Bob." Is this an e-mail from Uncle Bob? Or maybe it's from your co-worker? You don't know, and the spammer counts on your curiosity.

I don't want someone to think I am doing something inappropriate because I keeping getting these spam messages!

Unfortunately, in today's communication environment, spam is a fact of life, something we all try to avoid, but it comes anyway. None of us have any control over what is sent unsolicited to our inboxes, and while it may sometimes be offensive or embarrassing, it is out of our control to stop it; so understand that being the target of a spam message is in no way reflective of you as an employee, or as a person.

I received an email that was spam! Why didn't the filter catch it?

No spam filter is 100% perfect. Some spam will get by the filter and some legitimate mail will get tagged as spam. If we make the spam filter too aggressive then more legitimate mail will be trapped by the filter and deleted. Thus, we have to compromise and soften the spam filter a little in order to avoid catching as much legitimate mail as possible.

Even with a very aggressive filter, spam will still get through because filters are just computer programs that can only make educated guesses based on prior knowledge. We are constantly updating our filter to trap new versions of spam. Unfortunately, the spammers are constantly changing their methods to get around spam filters. Therefore, you may notice a sudden increase of a certain type of spam and then over time a decrease as the filter is adjusted.

Our spam filter is currently filtering out about 80 – 90% of all incoming messages as spam – all incoming messages. Our quarantine folder generally holds close to 150,000 blocked messages at any given time.

I received pornographic spam! Shouldn't the spam filter block pornography?

The spam filter does not specifically look for pornographic spam nor does it know what pornography is. The spam filter can only look for patterns which are typical of spam in general. Some of these patterns will include words and phrases typically found in pornographic messages. If enough spam patterns are found then the message will be blocked by the filter.

Should I reply to spam?

Never reply to spam or click on any link in a spam that claims to remove you from their mailing list. Often, doing this will just verify that your email address is active and will get your address added to even more spam mailing lists.

How did spammers get my email address?

There are a variety of ways that spammers can get your email address, including:

- Use web-crawling programs that look for mailto: codes in web pages
- Rip them out of online "white pages" directories
- From web forms you fill out asking for your email address (even some businesses may sell your email address)
- Buy a list of email addresses from someone (including businesses who may sell your email address)
- From mailing lists (some mailing lists will give out a list of all subscriber addresses).
- Take them from you without your knowledge when you visit their web site (for the latest on web browser security issues, see <http://www.cert.org/>).
- Run programs that collect email addresses from Web based discussion boards or Usenet postings
- From IRC or other chat rooms (such as AOL)
- Guess your email address (this is why it is important that you do not reply to spam so the spammers don't know that they guessed correctly).
- Somebody has your email address saved in their address book and their computer becomes infected with a virus which then harvests your address from their address book.

I keep getting multiple spam messages from the same person, or place, what can I do?

If you are getting several messages a day / week from the same sender. Send the address that you are receiving the spam from to - helpdesk@xenia.k12.oh.us We will add the address to our block filter. Also enable Junk Mail Handling on your GroupWise client (more later). Do not reply to the message! As much as you may want to 'give them a piece of your mind!'

I think that my legitimate mail is being filtered as spam, how do I know?

If you think you are not receiving mail from a sender, first contact them by phone, and or another email system (outside school) and verify that mail was sent. Verify that they have the correct address, and send them a message and ask that they reply. Many times we find that the sender has the wrong information, or has not actually sent an email. If this has been done, and you are still not receiving email, then contact helpdesk and we will check your account quarantine. This must be done within 7 days; our filter deletes quarantined messages after 7 days.

There are other filters and or blockers that may be stopping the mail also, either at the senders end, or between there and here, sometimes finding out what or who is blocking the mail is difficult.

People are telling me that my messages are not getting to them.

Though we have the ability to filter outgoing email, we do not. However, the same thing that you would do for not receiving mail needs to be done for sending mail problems, to resolve the issue.

How does our spam filter fight spam?

XCS has a dedicated server that runs a product from Computer Associates called eTrust. This product has three main components; ITM (anti-virus), Pest Patrol (anti-spyware), and SCM (anti-spam).

eTrust SCM's main spam filter, is the Advanced Spam Filter. This spam filter uses advanced technologies to analyze email messages. Bayesian and other mathematical analysis models are used to rate each email message with a score between 1 and 100. The higher the score, the higher the probability that the specific message is a spam email

By applying a spam probability score to each message, and allowing the eTrust SCM administrator to define flexible rules based on the spam score, a high level of spam detection is achieved. By default, eTrust SCM ships with a rule that tags any message with a score of 90 or higher as spam. The administrator can change this value based on local needs.

To allow a continued high spam detection rate, the Advanced spam filter signatures are updated as frequent as once an hour.

Additional spam detection layers include the following:

- Analysis of the entire email header, body, or both for keywords or phrases listed in a spam word list. The keywords search is made with a powerful regular expression engine helping you define extended phrases to fight spam.
- Real-time queries to real time black-hole list (RBL) providers to see if the sender is registered as a spammer.
- A local deny list of email senders, mail servers, relays, and domains that the administrator can ignore for a configurable period. .

Prevention

- **Block images in HTML messages that spammers use as Web beacons** A Web beacon can be a graphic image, linked to an external Web server, that is placed in an HTML-formatted message and can be used to verify that your e-mail address is valid when the message is opened and images downloaded.

GroupWise is set to Warn about HTML images by Default. If you are automatically seeing images in email messages, you may have inadvertently changed this setting. To see and or change the setting, in GroupWise, go to Tools> Options > Environment > Default Actions, and under HTML external Images, choose Always show warnings.

Remember, GroupWise only Warns you about the image, if you choose to view an image in an email, and click the information bar, then make sure it is from a trusted source.

- **Limit where you post your e-mail address** Be cautious about posting your e-mail address on public Web sites, and remove your e-mail address from your personal Web site. If you list or link to your e-mail address, you can expect to be spammed.
- **Disguise (or "munge") your e-mail address when you post it to a newsgroup, chat room, bulletin board, or other public places** For example, you can give your e-mail address as "s0me0ne@example.c0m" by using the number zero instead of the letter "o." This way, a person can interpret your address, but the automated programs that spammers use cannot.
- **Use multiple e-mail addresses for different purposes** You might set up one for personal use to correspond with friends, family, or colleagues, and use another for more public activities, such as requesting information, shopping, or for subscribing to newsletters, discussion lists, and newsgroups.

Everyone should have at least one free email account that is used for those times when you are required to enter an email address on a web form. You can sign up for free accounts at many places. Google, Yahoo, and MSN / hotmail, are all popular.

Your XCS email account should be reserved for work related business communication only.

- **Review the privacy policies of Web sites** When you sign up for online banking, shopping, and newsletters, review the privacy policy closely before you reveal your e-mail address and other personal information. Look at the Web site for a link (usually at the bottom of the home page) or section called "Privacy Statement," "Privacy Policy," "Terms and Conditions," or "Terms of Use." If the Web site does not explain how it will use your personal information, think twice about using that service.
- **Watch out for check boxes that are already selected** When you buy things online, companies sometimes add a check box (already selected!) to indicate that it is fine to sell or give your e-mail address to other businesses (third parties). Clear the check box so that your e-mail address won't be shared.
- **If a company uses e-mail messages to ask for personal information, don't respond by sending a message** Most legitimate companies will not ask for personal information in e-mail. Be suspicious if they do. It could be a spoofed e-mail message meant to look like a legitimate one. This tactic is known as "phishing" because, as the name implies, the spam is used as a means to "fish" for your credentials, such as your account number and passwords that are necessary to access and manipulate your financial accounts. If the spam is from a company that you do business with — for example, your credit card company — call the company, but don't use a phone number provided on the e-mail. Use a number that you find yourself, either through directory assistance, a bank statement, a bill, or other source. If it is a legitimate request, the telephone operator should be able to help you.
- **Don't contribute to a charity based on a request in e-mail** Unfortunately, some spammers prey on your good will. If you receive an appeal from a charity, treat it as spam. If it is a charity that you want to support, find their number elsewhere and call them to find out how you can make a contribution.
- **Don't forward chain e-mail messages** Besides causing more traffic over the line, forwarding a chain e-mail message might be furthering a hoax, and you lose control over who sees your e-mail address.
- **Never buy anything advertised in spam.** Even if you happen to be looking for a lower mortgage rate, don't look for it in junk e-mail. Chances are the services advertised are bogus anyway. Respected loan companies don't randomly flood inboxes.
- **Update your address book.** Make sure that the people you want to have contact with are in your address book: your friends, family, business associates, and companies you've requested e-mail from.
- **Turn on Junk Mail Handling.** GroupWise Client has a Junk Mail Handling tool that allows the user to block mail that may still get through the filter system. To access the tool, from within the GroupWise client, go to Tools> Junk Mail Handling.
 - Check the box marked "Enable Junk List",
 - Check the box marked "Enable Block List".
 - Optional, Check the box marked "Automatically delete items [# of days] after delivery".
 - Caution: Checking the box marked "Enable Junk Mail using address books", will cause mail from any sender you have NOT previously gotten mail from to be treated as junk mail, and any mail you have received, EVEN from spammers, to be allowed through.