University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

CU eComm Program

Permanent Email - Spam and Spoofing

We get a lot of inquiries regarding SPAM. As a result, we have compiled a list of the most frequently asked questions with explanations for each. See below. I hope you find this information helpful.

SPAM FAQ Is the alumni association sending me spam? No. Neither the alumni association nor Harris Internet Services, who host the Alumni Connections servers that maintain the email forwarding service, are the source of the spam. We respect your privacy and do not sell, or otherwise distribute, alumni email addresses; nor have they been stolen.

How did the spammers get my address? Unfortunately, there are many ways that spammers obtain email addresses: addresses compiled by commercial entities from web commerce; web crawlers searching for specific domain names (such as @alumni.anyschool.edu) on any web site where contact information might be listed; and a practice sometimes called "blind spamming" or "dictionary spamming" in which spammers simply guess at the username before the @ sign and send literally thousands of messages. This is why you may see a message addressed to "albert@, allen@, andrew@ ...," etc. The spammers run what is basically a dictionary of usernames against a domain - those that don't immediately bounce are kept and reused. This can give the false impression that the spammer has access to the list of user accounts. Viruses can also generate unwanted email and harvest addresses for spammers. Even if your computer is not infected, if someone else has your address in their address book and their computer becomes infected, viruses will often send multiple messages to everyone in the address book. It can also collect these addresses and send them to a spammer for later use.

Why does the spam look like it's coming from the alumni association or Alumni Connections? Every server that handles a piece of mail leaves a time stamp on it indicating when it processed the email. Since the Alumni Connections servers host the forwarding service for us, they are the last party who handles the email before it reaches your inbox. This does not mean that the spam originated from them, only that they are forwarding all mail sent to you.

What is spoofing? Spoofing is forging an email header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP (Simple Mail Transfer Protocol) -- does not include a way to authenticate. There is an SMTP service extension that allows an

SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information. This is very easy for SPAMmers to do because they often have their own mail server or use an ISP that doesn't verify email headers before sending them on the Internet.

Are the email forwarding servers secure? Yes. Periodic security and performance reviews are performed.

Does the alumni association or Alumni Connections filter out spam? Yes. Spam filters are employed that look at the spammer's IP address (the address of the server from which they send their messages) and name. The filters are constantly updated and filter out hundreds of spam messages a day. However, because our service only forwards email and does not store it for retrieval like your ISP, we must err on the side of caution in not wanting to filter out too much mail. In considering the nuisance caused by spam, we also have to consider the importance of your real email and make sure it is delivered to you in a timely fashion. For best results, you should contact your ISP regarding any available anti- spam measures. In the end, we hope that the advantages of using email, including the permanent email forwarding service, will continue to outweigh any drawbacks, including spam.

How can I prevent getting spam? There is no way to prevent all spam; but there are steps you can take to decrease the level and annoyance of spam. You should contact your Internet Service Provider (ISP, the company that provides your email service) and inquire about any anti-spam measures they offer. Most ISPs will help you set up filters that can be very effective at catching most spam. These filters can work even on messages sent to a forwarding address because they look at the message's internet header information and not just the From: field. Your ISP can advise you on what measures are available.

What should I do if I receive spam sent to my forwarding address? We try to be vigilant in combating spam, reporting all violations to the Alumni Connections system administrators and having them review the headers to be added to their spam filters. If you wish, you may forward to feedback@alumniconnections.com copies of any spam you receive and we'll pass them along to the administrators. Just be sure to include the full internet headers. Simply forwarding the message is not sufficient. You must include the full headers from the original email message.

What are internet headers? In addition to the usual To:, From:, and Subject: fields you see in your email, every message also carries detailed information about its route along the internet from sender to recipient. And every mail server it passes through puts a time stamp on it, indicating when it handled the message. Most email programs hide this information from plain view because it's not necessary or important for everyday email use. But it's always there in every message. And while it may look like undecipherable gibberish, it can tell an email administrator where the message came from and allow them to block that sender. Each email program stores them slightly differently.
Why am I getting so much more spam than ever before? Spam in general has increased exponentially in the past 2 years. There is, simply put, more spam being sent than ever before, so everyone is going to receive more of it. Additionally, university postmasters have noted that .edu domains in general

are also being targeted much more aggressively than just a year ago. This increase in spam does not mean, however, that our email administrators are falling down on the job. It means there is more spam out there, and we're getting some of it. At this point in time, unfortunately, receiving spam is all but inevitable for any email address.

Should I respond to spam or use their opt-out links? Generally speaking, the conventional wisdom still holds that it is best not to reply directly to spam. Doing so will only verify that your address is valid and may precipitate more spam. This is certainly the case with spam from unknown parties containing offers for which you have no interest (e.g., mail-order diplomas, pharmaceuticals, etc.). Of course, if you receive an email from a known source, such as an organization with which you are affiliated or an online vendor with whom you do business, you may be safe in responding. In general, common sense and healthy skepticism are usually sufficient in differentiating the kind of email you receive.

Why do I get email that says I sent a message with a virus when I know my system is clean? Many of the computer viruses in circulation will collect email addresses from an infected computer's address book and send them messages (and copies of the virus). The virus will also change the From: address to one of those in the address book. So if someone has your name in their address book and their computer becomes infected with a virus, their computer can send out messages with your address in the From: field. And if anyone replies to that message, it will come to you.

» »