

Spam

Unwanted commercial email, also known as "spam", can be annoying. Worse, it can include bogus offers that could cost all of us time and money. Our conference technology specialists work hard to limit the amount of spam that makes it to your inbox. However no system is 100%. And, there will be times when you get spam. At that point, there are some additional steps that you can take to help alleviate future occurrences. This is a quick video that will help you with some of the “techie” stuff you can do. And, in addition to that, here are some other things that you can do to prevent it from happening.

Limit your exposure. Never Use Your UMCNEB email address for personal shopping or things of the sort.

As much as you may not want to, you might decide to use some non-work email addresses — one for personal messages and one for shopping, newsletters, chat rooms, coupons and other services. You also might consider using a disposable email address service that forwards messages to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without affecting your permanent address.

Also, try not to display your email address in public. That includes on blog posts, in chat rooms, on social networking sites, or in online membership directories. Spammers use the web to harvest email addresses.

Check privacy policies and uncheck boxes.

Check the privacy policy before you submit your email address to a website. See if it allows the company to sell your email to others. You might decide not to submit your email address to websites that won't protect it.

When submitting your email address to a website, look for pre-checked boxes that sign you up for email updates from the company and its partners. Some websites allow you to opt out of receiving these mass emails.

How Can I Help Reduce Spam for Everyone?

Hackers and spammers troll the internet looking for computers that aren't protected by up-to-date security software. When they find unprotected computers, they try to install hidden software – called malware – that allows them to control the computers remotely.

Many thousands of these computers linked together make up a “botnet ,“ a network used by spammers to send millions of emails at once. Millions of home computers are part of botnets. In fact, most spam is sent this way.

Don't let spammers use your computer.

You can help reduce the chances that your computer will become part of a botnet:

- **Use good** computer security practices **and disconnect from the internet when you're away from your computer.** Hackers **CANNOT** get to your computer when it's not connected to the internet.
- **Be cautious about opening any attachments or downloading files from emails you receive.** Don't open an email attachment — even if it looks like it's from a friend or coworker — unless you are expecting it or you know what it is. If you send an email with an attached file, include a message explaining what it is.
- **Download free software only from sites you know and trust.** It can be appealing to download free software — like games, file-sharing programs, and customized toolbars. But remember that free software programs may contain malware.

Detect and get rid of malware.

It can be difficult to tell if a spammer has installed malware on your computer, but there are some warning signs:

- Your friends may tell you about weird email messages they've received from you.
- Your computer may operate more slowly or sluggishly.
- You may find email messages in your sent folder that you didn't send.

If your computer has been hacked or infected by a virus, disconnect from the internet right away. And contact the conference or district office for help removing the malware.

Report Spam

Forward unwanted or deceptive messages to:

- the Federal Trade Commission at spam@uce.gov. Be sure to include the complete spam email.

If you try to unsubscribe from an email list and your request is not honored, file a complaint with the FTC at <http://www.ftc.gov/complaint>.