Spam…Junk Email and Texts

What is spam?

It is annoying commercial electronic mail and text messages sent, often in bulk, to consumers without the consumer's prior request or consent. The goal of spam is to catch your eye.

Often spam is promoting get rich quick schemes and questionable products. Common scams are chain letters, work at home schemes, weight loss potions, credit repair offers, advance fee loans, vacation offers, and adult entertainment.

Do not give personal information out in response to a text.

Another common problem is "phishing," where the spammers are trying to get personal information from you.

Why do I get spam?

For the same reason you get junk mail through the Postal Service – people are trying to sell you things. Email is cheaper to send, so you get even more of it! Spam mailing lists are created in a variety of ways, including scanning discussion groups, buying or stealing Internet mailing lists, searching the Web for addresses, and even just guessing email addresses at random. If you use email, you will likely get spam.

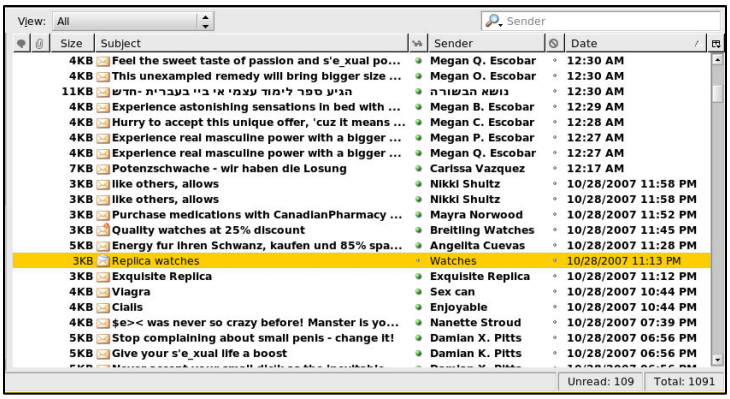
Is it spam? If you asked for it, it is not spam. For example, if you opt to receive emails from an online retailer, then those emails are not "spam" – at least not until you ask the retailer to stop emailing you.

Friends do not usually send spam. What if a friend forwards an email and asks you to send it to 10 other people? Ask them not to send you those emails.

Spam fighting tips

Get a spam filter

Many Internet Service Providers offer spam filters. You can usually activate one with a phone call to your provider or by updating your settings. However, not every spam filter is perfect. The best filters still mark some spam as legitimate messages, and accidentally mark some legitimate messages as spam.



Wikimedia Commons

Never reply directly to spam

A reply, even requesting to be deleted or removed from a mailing list, verifies to the spammer that your email address is active. You may end up getting even more spam.

Do not open your spam

Some spam messages are programmed to notify the sender when the email has been opened. Then, spammers know your email address is valid and active. Additionally, if you open up an email you risk exposing your computer to a virus. Delete spam without opening it.

Do not post your email address on a website, newsgroup or display in public; that includes on blog posts, in chat rooms, on social media sites, or in online membership directories. Spammers use email robots to collect addresses from newsgroups and the Web.

Confuse spammers

by using two email accounts. Give your primary account to friends, family, and colleagues. Use the other account (you can get a free email address that is accessible online) for mailing lists, shopping, newsgroups, or Web forms.

Choose a unique email address

Your choice of email addresses may affect the amount of spam you receive. Spammers send out millions of messages to probable name combinations at large ISPs and email services, hoping to find a valid address. Thus, a common name such as jdoe may get more spam than a more unique name like j26d0e34.

Check a website's privacy policy

before giving your email address. Most often you can find a link to the company's privacy policy, which is usually located at the bottom of the web page. If you are still confused about their policy, email and ask:

- How does the company use the information you share with them?
- How do they protect children's privacy?
- Do they share information with a third party?
- How do I access the information to change or delete it from the company's database?
- How do I remove my information from email, phone, and postal mailing lists?

Screen spam.

You can program your email to filter out messages that have subject lines in all caps, a dollar sign or exclamation points, words like "unsubscribe," "X-priority," "adv," "bulk email," or "make money fast" in subject lines. Most filters let you select people or words to always allow through.

Be skeptical of commercial email

Do not believe promises from strangers. Greet money making opportunities with skepticism. Most of the time, these are old scams delivered through the newest technology.

Do not let spammers use your computer

Use good computer security practices and disconnect from the internet when you are away from your computer. Hackers cannot get to your computer when it is not connected to the internet.

Be cautious about opening any attachments or downloading files from emails you receive. Do not open any email attachment-even if it looks like it is 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.

Check out

dmachoice.org

This site allows you to "opt out" of national email lists, which will limit the amount of unsolicited emails you receive.

- Text message spam is a triple threat. It often uses the promise of free gifts, like computers or gift cards, or product offers, like cheap mortgages, credit cards, or debt relief services to get you to reveal personal information. If you want to claim your gift or pursue an offer, you may need to share personal information, like how much money you make, how much you owe, or your bank account information, credit card or Social Security number. Clicking on a link may install malware that collects information from your phone. Once the spammer has your information, it is sold to marketers, or worse, identity thieves.
- It can lead to unwanted charges on your cell phone bill. Your wireless carrier may charge you simply for receiving a text message, regardless of whether you requested it.
- It can lead to slow cell phone performance by taking up space in your phone's memory.

Text message spam is illegal under federal law (15 U.S.C. ch. 103)

It is illegal to send unsolicited commercial email messages to wireless devices, including cell phones and pagers, unless the sender gets your permission first. It is also illegal to send unsolicited text messages from an auto-dialer-equipment that stores and dials phone numbers using a random or sequential number generator, 47 U.S.C. § 227(b)(1)(a).

Exceptions to the law (15 U.S.C. § 7702):

- Transactional or relationship types of messages. If a company has a relationship with you, it can send

you things like statements or warranty information.

- Non-commercial messages. This includes political surveys or fund-raising messages.

Can the spam

Here are a few steps to can text message spam:

- Delete text messages that ask you to confirm or provide personal information. Legitimate companies do not ask for information like your account numbers or passwords by email or text.
- Do not reply and do not click on links provided in the message. Links can install malware on your computer and take you to spoof sites that look real but whose purpose is to steal your information.
- Treat your personal information like cash. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. Do not give personal information out in response to a text.
- Place your cell phone number on the National Do Not Call Registry at:

  donotcall.gov

- If you are an AT&T, T-Mobile, Verizon, Sprint or Bell subscriber, you can report spam texts to your carrier by copying the original message and forwarding it to the number 7726(SPAM), free of charge.

Complain about spam

Send a copy of the unwanted or deceptive message to the Federal Trade Commission (FTC) at:

spam@uce.gov

The FTC pursues law enforcement actions against people who send deceptive spam.

When you complain, it is important to include the full email header. The information in the header makes it possible for consumer protection agencies to follow up on your complaint.

Finding the header

Search the help function of your email program with the term "view header." If you are unable to find information in the program's help file, you may want to search the internet for the term "header" along with your email program.

Send a copy of the spam

to your Internet Service Provider (ISP). This lets them know about the spam problem and helps them to stop it. Make sure to include a copy of the spam, along with the full email header. Start at the top of the message that you are complaining about spam.

You also may want to complain to the sender's ISP because most ISPs want to cut off spammers who abuse their system.

SpamCop.net

This website offers a free spam-reporting service that will automatically detect the illegitimate headers and send a form complaint to the proper authorities.

More help

To learn more about or get help fighting spam, check the following websites:

Federal Trade Commission
ftc.gov

Direct Marketing Association
dmachoice.org

For information on current spam laws within the United States:

spamlaws.com

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

Spam284 (rev 9/19)