The term "spam" refers an unsolicited email message from a sender you don’t know. Spam messages are usually sent in bulk to numerous recipients with all of the messages having substantially identical content. Spam is sometimes called "junk mail" or "unsolicited bulk email".

There are two types of spam:

(1) **nuisance** emails, such as solicitations to buy products or services; and
(2) **malicious** or **phishing** emails, which may try to trick you into revealing personal information that then can be used to defraud you.

While nuisance spam is the most numerous and annoying type of spam, malicious or phishing email is potentially the most dangerous. It is often difficult to distinguish between a message intended to defraud you and a legitimate one. For example, legitimate email messages from Marriott to its customers after a data breach did not look legitimate.

With phishing, consumers receive messages from dishonest sources disguised as email from trusted retailers, financial institutions, or even government agencies. Most phishing emails seek to obtain the consumer’s personal information, such as passwords, personal identification numbers (PINs), Social Security numbers and account numbers. Phishing emails can often lead to data breaches at organizations.

The federal **CAN-SPAM Act** (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) does not ban spam per se. Instead, it prohibits deceptive or misleading commercial email, requires senders to provide recipients with the ability to "opt out" of future mailings, and imposes a variety of other requirements. These requirements vary depending on whether the email is categorized as a commercial message or a transactional or relationship message.

The CAN-SPAM Act sets forth the basic legal principles that differentiate legal and illegal commercial email. Technically, the CAN-SPAM Act doesn’t apply just to bulk email. It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service".

---

**Tips for Dealing With Spam**

- **Never open spam messages.** Unless you block HTML graphics in your email program, the sender can be alerted that you have opened the message. This encourages spammers to send more messages.
- **Never click on a link** in a spam email. This could alert the site to the validity of your email address, potentially resulting in more spam. It could also expose your computer to malware. Scam email messages often give a link that includes the name of your bank, a government agency or another legitimate source. Clicking on the link may direct you to a counterfeit site that could look like the official site.
- **Never reply to a spam message.** That informs the spammer that you exist. Responding to the messages just confirms that your email address is valid and that you received and read their message. It also encourages them to send more messages. Don’t respond to any “removal instructions” that might be included at the bottom of the message. Common sense says a company that uses fraud and deception in its solicitation is unlikely to take your opt-out request seriously.
- **Set filters in your email program to allow or to block specific senders and/or specific language.** Email filters can be set to keep out certain senders, or conversely, to "white list" other correspondents by allowing their specific email address. If you find that either legitimate messages are being captured in your spam filter or that unwanted messages are continuing to slip through to your inbox, you may need to adjust the spam filter settings.
- **Understand where rejected messages go.** If you use filtering software, be sure the rejected messages are sent to a special folder other than your email "trash" folder. That way you can periodically review them to see if a message you truly
want was diverted by an overly-aggressive spam filter.

- **Have a backup email account(s).** Use a free online email account when subscribing to magazines, filling out warranties, posting to online discussion groups, or in other situations where you are not sure how your email address will be used. While this won’t reduce the amount of spam you receive, it will keep it out of your primary email account that you use on a daily basis.

- **Consider using disposable online addresses.** You can create a unique email address for each email newsletter or forum you subscribe to. Then, when an email address begins getting spam, you can discontinue using it and start using another. This works because the disposable email addresses actually forward to your real email address.

- **Be cautious when making online purchases.** Read online and offline forms carefully and check or uncheck boxes as necessary to make sure you are not inadvertently giving your consent to receive spam. Every reputable site offers information about how it processes your order. It is usually listed in the section entitled Privacy Policy.

---

**Resources**

- FTC Consumer Information: Spam [6]
- FTC Consumer Information: Phishing [7]
- U.S. Department of Justice [9] (for reporting spam)

---

**Source URL (modified on December 10, 2018):** https://www.privacyrights.org/consumer-guides/anti-spam-resources

**Links**