Spam

Share this page

Unwanted commercial email – also known as "spam" – can be annoying. Worse, it can include bogus offers that could cost you time and money. Take steps to limit the amount of spam you get, and treat spam offers the same way you would treat an uninvited telemarketing sales call. Don't believe promises from strangers. Learn to recognize the most common online scams.

How Can I Reduce the Amount of Spam I Get?

Use an email filter.

Check your email account to see if it provides a tool to filter out potential spam or to channel spam into a bulk email folder. You might want to consider these options when you're choosing which Internet Service Provider (ISP) or email service to use.

Limit your exposure.

You might decide to use two 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.

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. Of course, there is a downside - it's harder to remember an unusual email address.

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 can't 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. Then take steps to remove malware.

Report Spam

Forward unwanted or deceptive messages to:

- your email provider. At the top of the message, state that you're complaining about being spammed. Some email services include buttons you can click to mark messages as junk mail or report spam.
- the sender's email provider, if you can tell who it is. Most web mail providers and ISPs want to cut off spammers who abuse their systems. Again, make sure to include the entire spam email and say that you're complaining about spam.

The FTC is working to keep your inbox clear of spam. In the past, the FTC asked you to help by forwarding the spam you received. Now, the FTC collects spam by using a honeypot, which is an online trap. This change makes it more efficient for the FTC to collect spam that is deceptive or illegal, saving tax dollars and your time.

If you lost money to a scam that started with an email, please report it at ftc.gov/complaint.

Read more about how to limit spam, phone calls, and mail.

Tagged with: computer security, privacy, scam, spam September 2011

Related Items

- How to Recognize and Report Spam Text Messages
- What to Do If You Were Scammed