
**Volume #4 - Issue #183**
**October 26th, 2018**
**This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.**

## How to Stop SPAM


Spam is everywhere and can definitely be one of the most irritating consequences of our digital world. It is very common through email, but unfortunately, text message spam is also growing rapidly. Hopefully the following information will help you decrease your spam in both formats. Short of cutting yourself off from the Internet, there's no way to eliminate email spam entirely. The best you can do is filter out most of it, and even that has some unfortunate consequences.

**1. Train your filter**

Your email client (the local program or cloud-based service you use to access and send email) almost certainly filters spam, moving suspicious messages to a separate folder. When you find spam in your inbox, don't just delete it. Select it, and tell your mail client that this particular message is spam. How you do this depends on your client. For instance, if you're using Gmail's website, click the *Report spam* button in the toolbar (the icon looks like an exclamation point inside a stop sign). But it's not perfect. Some spam tricks the filter and ends up in your inbox, and some legitimate messages, called false positives, end up in the spam folder. You also need to train the client about your false positives. Once a day, go through your spam folder looking for messages that don't belong there. When you find one, select it and tell the client that it made a mistake. In Gmail, you click the *Not spam* button. If your mail client is halfway decent, it will learn from these mistakes…but only if you train it.

**2. Never respond to spam**

If you recognize something as spam before you open it, don't open it. If you open it and then realize it's spam, close it. Do not click a link or a button, or download a file, from a message that you even *remotely* suspect is spam. If you opened a spam because it appeared to be coming from a friend or co-worker, contact them immediately and let them know that their account has been compromised.

**3. Hide your email address**

The more people who have your email address, the more spam you're going to get. So keep your address close to your chest. Don't publish it on the web unless you absolutely have to. (I have to, and it's not fun.) And if you have to, use a different address for that purpose. Use disposable email addresses when you're not comfortable sharing your real one. It is easy to

set up free email addresses using almost any service. (Gmail, AOL, Yahoo, etc.)

**4. Use a third-party anti-spam filter**
Most of the major security suites come with an anti-spam filter that can augment the one on your client—but only if that client is local. In other words, they can work with Office's Outlook program, but not with outlook.com.

**5. Change your email address**
This is a very drastic option, but if you've responded to spam in the past or haven't hidden your address, and are therefore overloaded with spam, it may be your best option. Of course you'll have to inform your legitimate contacts about the change, and you'll probably have to keep both addresses for a few months. But once you can get rid of the old address, your spam count should plummet. As said early, it is becoming more common to be blasted by spam text messages that are either seeking to sell them something or, even worse, steal their personal information. But in a recent report, the Federal Trade Commission (FTC) is reminding everyone that they don't have to take these messages lying down. The agency points out that spam text messages are often illegal and that consumers need to be careful about how they handle them and what information they reveal. Text message spam can be a triple threat: it often uses the promise of free gifts or product offers to get you to reveal personal information; it can lead to unwanted charges on your cell phone bill; and it can slow cell phone performance..

The FTC notes that unsolicited commercial email messages or text messages to wireless devices are illegal under the Telephone Consumer Protection Act (TCPA). There are a few exceptions – such as if the sender

has a relationship to the recipient or if they come from political or fundraising organizations – but for the most part consumers need to give their consent before they can legally receive messages.

However, as many of us are aware, that doesn't stop companies or individuals from sending them. To protect yourself from text message spam, the FTC offers the following tips:

**1. Delete text messages that ask you to confirm or provide personal information:** Legitimate companies don't ask for information like your account numbers or passwords by email or text.

**2. Don't reply, and don't click on links provided in the message:** Links can install malware on your computer or device and can take you to spoof sites that look real but whose purpose is to steal your information.

**3. 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. Don't give them out in response to a text.

**4. Put your cell phone number on the National Do Not Call Registry.**

**5. Report spam texts** to your carrier by copying the original message and forwarding it to the number 7726 (SPAM), free of charge.

**6. Reviewing your cell phone bill** for unauthorized charges, and reporting them to your carrier.

The FTC also asks that consumers who receive unwanted commercial or regular text messages file a complaint with the agency at this link: **https://www.ftccomplaintassistant.gov**

**Thank you for subscribing to our email!**