

## What the Tech?!: Spam by Joe McCormick

Chances are your email service has a folder labeled “Spam.” Spam is defined as information being repeatedly sent under the false pretense that the information is useful to you. In fact, most spam is based on advertising or phishing scams. But don’t be fooled, the dangers of spam are very real. Every year, thousands of people are scammed out of millions of dollars across the world. Estimates of the actual losses suffered range anywhere from 50 million to 3 billion dollars annually. It is very important to be aware of spam, what it looks like, and how it can be avoided.

Every now and then our email filters may fail, allowing a piece of spam to get into our main inbox. Here are some tips that can keep you protected. When viewing the email, you should be able to see the sender’s address, “wtt.globe@gmail.com” for example. You want to focus on the domain name of the address, in this case, “gmail.com.” If the domain name is not familiar to you or is just a random mix of numbers and letters, it is most likely spam.

The next major indicator is how the email is worded. A significant amount of spam is sent from outside the US by people who speak English either poorly or not at all. They will write the email in their native language and then put it through a translator. What generally comes out of a translator is poorly constructed and easy to spot as spam.

Some other spam techniques are more obvious. If the message is written in all capital letters or colored text, it is very likely spam. However, the biggest sign is the content of the message. If it is asking you to visit another website, donate to an obscure foundation or cause, asking for money in general, offering money to you, or wanting you to give up any personal information, it is most certainly spam.

The most famous example is probably the “419 Fraud,” better known as the “Nigerian Businessman Scam.” This scam has been around since the ‘80s and is based around a story that has sapped millions from citizens all across the world. You’ll get an email from a Nigerian “official” who says they are being cheated out of their hard-earned millions. All they want to do is deposit the money into your bank account, come safely to America, and be given back their money minus your service fee. Trouble arises when you end up having to “bribe” people in the process in order to seal the deal. Some have even traveled to Nigeria in order to make sure everything went smoothly. A small few of these people wound up being kidnapped for a ransom. So you can see why it’s important to be aware of these scams.

Spam does not just come in the form of emails, however. Advertisements on the web are becoming increasingly invasive, some even targeted to our specific interests. I’m sure most of you have been tempted by the allure of the “free iPod, just fill out these surveys!” Well, there is no free iPod, sorry to say. As you can see on most websites, these advertisements come to us in the sidebars or tops or bottoms of pages with flashy graphics, or fun mini-games, and sometimes even deafeningly loud sounds. Luckily, there is a super-effective way to deal with this kind of spam.

If you use the Firefox or Chrome browsers, you can download NoScript, a very handy add-on easily found on Google. NoScript is by far one of the most useful add-ons I have ever encountered as it basically removes all third-party scripts on every website, allowing you to simply view the content. A “script” is the programming code used to create what we see on a website. There are slight drawbacks if you’re trying to use a media-based website, as NoScript will block the scripts for audio, video, and flash, among others. However, NoScript runs off of a filter, so you can simply allow entire websites to run their scripts; this filter can be accessed by clicking on the “S” in the lower right corner of your browser. Over time you will allow scripts from the websites you repeatedly visit and this issues goes away, allowing for an advertisement-free browsing experience. I hugely recommend it.