To Unsubscribe or Not…THAT is the Question

The Situation

We've all experienced this… an email shows up in your Inbox from a company you've never heard of. It's obviously a marketing email – they're talking to you like you're a long-lost rich relative and they want to make sure you're aware of all the features of their shiny new version 2.0 Widget. You've got no interest in a 2.0 version Widget so you delete it, and move on thinking that you've dealt with that little problem.

Not so fast…. A couple of days later, you get another email from the company, this time trying to arrange an appointment so that they can personally introduce you to Widget 2.0. "Enough is enough… I don't want any more of these emails" you think to yourself. "Ah… they've got an Unsubscribe link – I'll just click on that and put an end to this." But wait…is that really a good idea?

The Issues

Unfortunately, those handy little unsubscribe links can create more problems than they solve. Here's some things about using unsubscribe links to consider:

1. **You have confirmed to the sender that your email address is both valid and in active use.** If the sender has questionable ethics they will likely continue to send you spam. Worse still, they can sell your email address to other spammers.
2. **By responding to the email, you have positively confirmed that you have opened and read it.** The spammers now know that you are aware of what they're trying to promote. Even more reason for them to continue emailing you.
3. **If you respond by email, you've exposed information about your email software and your computer.** The common scenario here is "To unsubscribe, reply to this email with Unsubscribe in the subject line". The risk is that emails carry with them a lot of data about the email system that sends them (known as email headers) and this can be of value to the spammers.
4. **If you respond by opening a browser window, you're giving away more about yourself.** By visiting the spammer's website to "unsubscribe" you're giving them information about your location (they use your browser's IP address to work that out), your computer operating system, the browser you're using, etc. Oh, and they may download a "cookie" onto your system which may allow them to identify you if you visit any other sites they own.
5. **The scariest of all.** If you visit their website, you've given them an opportunity to install malware onto your computer. It's called a "drive-by" download and the spammers use the information you've shared to tailor the exploits they push out specifically to work with your computer.

What Should You Do?

We'll start with the simple answer and move to the "but what if's".

1. **Simple Answer: If the message is unsolicited, then mark it as "Junk".** Not only does this move the message to your Junk folder, but modern email software "learns" what you consider spam. It will get better at blocking messages in the future. How do you mark it as Junk? Right-click on the message, select Junk from the list and then click on Block Sender.
2. **But: If it's a newsletter or other communication from an organisation that you have or have had a relationship, then you can probably safely click on the unsubscribe link.**
    a. A good clue as to whether it's safe is to check and see if the message was sent through a well-known email system such as ConstantContact or Mail Chimp. If it was, then go ahead and click on the Unsubscribe link.
    b. Another indicator is where the Unsubscribe link goes to. If it links back to the sender's organisation AND it's a well-known / reputable company then you're likely safe. e.g. I'd click on an unsubscribe link from coca-cola.com, once I verified that it was indeed their link, but I'd run screaming from a link from JoesGarage_PawnShop.com. The challenge here is being able to decipher the link.
3. **If it becomes extreme.** We've had occasion where some spammers were inundating people with endless streams of junk email and nothing they could do would make it stop. If that happens to you, please contact Computer Help Desk. There are things we can do behind the scenes to deal with these extreme cases.

An Ounce of Prevention….

One of the best ways to prevent SPAM from showing up in your Inbox is to be careful about what you do with your email address.

1. **Treat your key email addresses as privileged information.** Be very careful about using your key email addresses – your business address, your primary personal email address, etc. Posting on public forums using these addresses is a guaranteed invitation to spammers. The same goes for creating accounts with sites you rarely use, companies you'll likely deal with only once, etc. I'm not saying don't do it but rather, consider who you're dealing with versus the risk of giving them important information.
2. **Consider getting a "throw-away" email address.** A throw-away email address is one you use for situations where you don't want to expose your primary email addresses. Public forums are a good example. Set up a Gmail address, use it as required and log into it periodically to clean out the junk. You'll be amazed at what you've collected.

Finally…

The final complicating factor in all of this has to do with the legislation around commercial use of email. Many countries, including Canada, have very specific rules about the use of email for commercial purposes. Unsubscribe links, time to process an unsubscribe request, consent to receive commercial emails, etc. are all part of it. However, some countries – notably the United States – do not have these requirements and thus you may occasionally receive a legitimate commercial message from a US-based organisation. Consider the sender, apply the guidelines listed above and act as you believe is appropriate.