Radio Days – 2012-07-07

Reducing Spam in Your Inbox

Spam. The very word sends some people into paroxysms of rage because they get so many unwanted emails that their world is going into overdrive just at the thought of getting their emails. You can change all this with very little effort and, for many people, no cost. Isn't that worth working toward?

There are several strategies to follow, and most of them are just plain common sense.

Do Not Click!

If you get an unwanted email **DO NOT CLICK** on any link in the message. There are a number of reasons for this piece of advice:

- You have just confirmed that your address is active. All spammers are looking for email addresses which are seen by a real live person. This is because such addresses are valuable. They are valuable for two reasons: the spammer can send more email to these addresses because someone is looking at the emails, and this address can be sold for real money. You may not think that your email address can have some value, but to spammers they are worth their weight in gold.
- You are likely to end up with an infected computer. This infection may, or may not, be obvious. A well written virus will not be obvious but will do its dirty work in silence so that you are unaware that you have been targeted by a virus. Lots of virus writers want the bragging rights which go with an infected computer, so the infection may be obvious. Only time will tell with your computer and your infection.
- Even if you do not click on a link in the email you can still get infected! This fact is not widely known, but that does not mean that it is not true. There is a technique which allows an email to send a reply to the sender without your knowledge. This works with small images which are not visible in the email but which do phone home and let the owner know that your email address is alive. The same technique can install a virus on your computer!

Guard Your Email Address

This is one of the most important pieces of advice that I can give you. You may have entered your email address into a website which promised to give you a benefit which you wanted. You may not have noticed that there was a little checkbox on the signup page which allows the website owner to send you lots more email. Sometimes this checkbox also authorises the website owner to allow affiliated companies to send you emails. Even worse, this checkbox can allow the website owner to sell your address to anybody willing to pay for it. This means that your address can go viral in a very short time.

As I have often advised people: RTFS (Read The Flaming Screen)!

Get a Dummy Email Address

Dummy email addresses are very useful if you need to sign up to something but do not want the website to know your real email address. Many websites want your email address for a good reason: perhaps they need to send you an invoice for your records or your flight booking so that you can board the plane for that wonderful holiday which you and your family have looked forward to for months. There could be very little that is more frustrating than getting to the airport and finding that you do not have your ticket with you!

There are, of course, times when you do not want the company to know your email address. For those times when it is not important that you get some acknowledgement of a request you can use either a throw-away email address or a dummy address which does not get back to you. You can easily create a single-use email address at one of the free email providers like Hotmail. This is an email address which you open for the duration of the transaction then

close. If you cannot remember either the email address or its password you will not go back to collect the spam.

Another option which I have used is a dummy email address. I often use the email address *donald@duck.com* because I like the sound of it. You could also use *mickey@mouse.com* or even *minney@mouse.com*! All these addresses may or may not work: this does not matter because they will not be used to annoy you!

Sometimes this technique does not work because you have to reply to an email which the website sends you to prove that you are a real person. This is the time when I find that a single-use (or throw-away) address is the best solution. To create a single-use email address go to one of the free email address providers and create an email address. You do not have to remember the password used to access this address because you are not going to use it again. After you have created this address you then complete the form on the website, respond to the email which will shortly arrive then close the free email webpage.

Ignore Chain Emails

One of the scourges of the modern world is the chain email. This type of email asks, or even implores, you to pass it on to everybody that you have ever met. There are many reasons why you should not respond to these emails.

- They clog up the internet. Some of these emails have been doing the rounds since last century! They lie dormant for a year or so then somebody finds one in their inbox and sends it to everybody that they know.
- The person who sent you this email sent it to almost everybody in their address book. Not only did they send it to everybody, they use the *To:* section of their email program so that everybody gets everybody else's email address. This is almost guaranteed to ensure that your email address is plastered over an infected computer and thus to a spammer's email list.

If you do send an email to a number of people then please follow these simple rules:

- Send the email to yourself. This sounds stupid but it is a good beginning.
- Now enter the addresses of all the people to whom you want to send the email into the *BCC:* address area. This means that each person who gets the email only sees your address and their own, so nobody's privacy is compromised.

BCC

BCC stands for *Blind Carbon Copy*. This is a technique used in the olden days of typewriters and carbon paper. If you are too young to remember carbon paper it is placed between sheets of paper so that the typing is printed on the top page by the typewriter and on the lower pages by the carbon paper. When writing a letter you may want to send the letter to a number of people. If you want people to know that this letter is being copied you would write *CC:* (for *Carbon Copy*) at the bottom of the page together with the names of the other people to get it.

If you want other people to get a copy of the letter without alerting the named recipients you would then just send a copy of the letter to another person without placing their name on any other person's copy. This is called a *Blind Carbon Copy* or *BCC*.

The *BCC:* address area of an email is used to send an email to many people while preserving their privacy. In the context of reducing spam this technique will also help preserve other people's inboxes from the dreaded influx of spam.

Please do your bit to reduce this menace.

Check All Emails Before Downloading

Once you have downloaded an email it can wreak its havoc on your computer. The solution is obvious: do not download the email. This seems to fly in the face of reason: how do you read an email to know whether or not you should download an email?

The answer is easy: use a program which allows you to check all your emails while they are still on the server and before they are downloaded. There is an excellent program which does just that: it is called *MailWasher*. This program comes in two versions: MailWasher Free and MailWasher Pro.

The free version checks just one email address while the pro version can check an unlimited number of email addresses. When you check your emails using MailWasher the email is still on the server so cannot harm your computer. Also, because the email is still on the server, you can bounce it. This fools the sender so he thinks that your address is not valid.

Bouncing an email is the electronic equivalent of writing on an envelope *Not at this address: please return to sender*. The returned email does stop most spammers from sending you more unwanted emails. It cannot completely eliminate all spam emails, but it will reduce the number quite considerably.

Using Gmail

Gmail, like all online email services, has an excellent spam detection and removal process. If you have an exceptionally large number of spam emails that you can create a Gmail account specifically to remove spam emails.

You then forward all your emails to your Gmail account. Because Gmail has such good spam-fighting tools you will lose around 95% of the spam emails which originally came into your account. Then, because Gmail can be used as a normal POP email account, you can use MailWasher to remove the few remaining spam emails as you would from a normal email account.

Then, using your normal email program, you can retrieve all your remaining, good emails from your Gmail account, reading and enjoying them without the effort of all the cleansing needed to get rid of the spam.

Summary

Just a few simple rules and you will be well on your way to enjoying an almost spam-free email experience. As with so many things, it is simple when you know how.

Further Information

MailWasher Free	www.mailwasher.net
MailWasher Pro	www.firetrust.com
Gmail	www.google.com/mail