

Article: [COMPUTERS BEHAVING BADLY](#)

Topic: Emails

Author: Mark Ahearn

At the start of 2005, the proportion of spam was just over 80% of all email traffic. At the start of 2001 that figure was just 8%. Sadly, spam is here to stay.

With the ever increasing annoyance of SPAM (unwanted emails) it is getting easier for the unwary computer user to be innocently misdirected by email claiming, for example, that your bank account is about to expire and to give them your password, or to click on the supplied link or button to download anti-spyware programs or to unsubscribe from getting this email again.

When dealing with unsolicited emails, your best defence is commonsense. That is, don't open emails that; aren't to your email address, aren't from someone you know or were expecting, claim to offer the world, ask for any sort of personal information, offer computer updates and patches via a link in the email, or any other marketing or advertising ploy.

Emails claiming to be from your bank or Microsoft are always hoaxes. Microsoft does not email their customers to inform them of latest news unless you have signed up to receive their regular newsletters. All Microsoft updates have to be 'gotten', they aren't sent to you in an email.

A good habit to get into is to make sure your antivirus program is updated before downloading your emails. We all jump on the web and the first thing we do is check our emails. This usually happens all before the antivirus program has had a chance to detect you are on the web and download any updates. If you had just come back from a 4 week holiday and start reading your emails, you could be using a virus definition set that is 4 weeks behind the latest threats. So an email with a latest viral infection will not be caught by your antivirus software.

The best method to deal with spam is to simply delete it and move on. Never reply to spam or try to unsubscribe as this just confirms your email to the sender and you will be flagged for even more spam. These people usually don't know they have successfully spammed someone. They use a program to randomly generate emails in the hope they eventually make a successful one or they use a list of email accounts they 'acquired'. Many of these emails are obsolete and your reply simple moves you off the 'maybe' list to the 'actual' list.

Spam goes in cycles. As your name appears on the lists, others are as well. Eventually this list gets so big that they can't be managed, either in sheer physical size or in the amount of computer time need to email all the recipients. Your name will eventually drop off the list through naturally attrition. Of course that's when it will probably appear on someone else's list!.

There is anti-spam software, but this usually makes as many hassles as it solves. There is the initial cost of the software, the regular updating, the user intervention in deciding who gets added to the 'black' list and the high chance that it will block email you actually wanted but still allow spam through due to the ingenious ways these people are spelling the keywords that anti-spam software looks for.

Remember – Curiosity killed the Computer.

mark@computersbehavingbadly.com