

You're about to get ripped-off!

Email is becoming increasingly difficult to tell the difference between legitimate "offers" and a scam rip-off. The old adage "If it doesn't sell, they don't keep advertising" is always true -- so it's obvious that unsolicited email (aka: UCE, Spam) must be working or they'd no longer be doing it. **So, all you folks out there who actually respond to Spam, please don't!!**

Here are Ten key rules to think about before you click the reply button:

1. If there are more than two slashes in the domain... delete it

Look at the domain. If you can count more than ONE slash after the dot-com, beware. All of the following said they would send me 25,000,000 email addresses on CD for just £199.00. Here's a flash: you can't get that many email addresses on a CD... SCAM. All four, and many others like them lead to dead ends, only wanting your money:

<http://homex.coolconnect.com/member3/justhits/>

<http://www.megspace.com/internet/justhits/>

<http://www.stas.net/3/justhits/>

<http://www.freehost.nu/members/justhits/>

(These are also freebie hosting sites, see 9 below.)

2. If the domain is numeric ... it's sure to be a scam!

Any self-respecting and on-the-level business, with an honest offer will NOT use an IP number instead of a URL address. Instead, they use these to avoid detection, and to rip you off... <http://207.173.123.243:524> spells trouble.

3. If they say use this or that ... use neither

Con artists these days know they'll be shut down -- it's only a matter of time. So in order to sucker in more people they'll list several domains, hoping you'll move to the second one if the first one already got shut down. Many even say, "If one doesn't work, use the other!" That's your cue to use neither.

4. Who sent it is not who gets it ... don't let them get you

Look carefully at the address of the sender. Now go through the piece and look at any email addresses in the post, including headers. If they're not the same -- beware! They should at least be from the same domain. (That's the part after the "@".)

5. No real name means no real person

dhckj@msn.com, i27452@compuserve.com? eyzjygeynf@yahoo.com ... who are they trying to kid? These addresses are generated by Spam robots who open accounts at the freebie web sites, send mass mailings, change the name, send more, then cancel the account before they're detected. They should be outlawed.

6. If they tell you to talk to a robot ... tell'em no!

Many get-rich schemers and rip-off artists today tell you to call their toll free number, leave your name, address and phone number so they can call you back. They prey on the very poor, and the elderly. Their yarn is convincing -- but don't expect them to call back... in reality all they want is to SELL your address to other marketers.

7. If there's no address... you don't want to go there!

Check the spammers web site for a physical address. If you don't find one, there's a reason why: they don't want to be tracked down by anyone who they've done wrong... most especially the FBI. If there's a phone number, call it. Ask for their address. A recent Spam from "Vortal Toner Supplies" absolutely refused to give an address -- another said they didn't give out the address to anyone no matter what. They turned out to be an illegal, offshore gambling operation owned by a company in LA. Never reply or buy.

8. If it's offshore money ... don't touch it!

If it has to do with money but they're from another country other than your own -- get away quickly. Email has exploded with insurance quotes, bogus stock tips, shady refinancing debt services or home mortgages from the likes of Great-Loan-Rates@6aaa.fsnet.co.uk, whpost10986@avtechk.com.cn. These people cannot fulfil their promises... they're ripping you off.

9. If they're using a freebie account... you can't afford it

If you think about it for a moment, it's rather obvious that you wouldn't want to do business with anyone using a freebie email account. If they've got nothing to lose, then they've got nothing for you! Several of those below admit openly that their clientele is 88% spammers. All of the following freebie sites are responsible for the majority of Spam:

angelfire.com	another.com	arabia.com	bangkok.com
building.com	china.com	consultant.com	email-prom.net
email.com	excite.com	golfmail.com	hotmail.com
iway2000.com	loudpages.com	lycos.co.uk	lycos.com
mail.com	megspace.com	metahoo.com	mundomail.net
netcolony.com	netdest.com	netnet.com.sg	newmail.net
oceanfree.net	postmaster.com	prontomail.com	telsurf.net
turbomail.net	usa.com	verizon.net	verizonmail.com
virtualactive.com	bigfoot.com	webmail.co.za	wickedspeed.net
yahoo.com	India.com	freehosting.com	

10. If it's too good to be true... it is!

The other day a Spam email told me I could look like Cindy Crawford in two weeks. (Picture that!) Another said I no longer had to worry about debts ... yet another said it could get me out of financial trouble... dozens of them each day want to sell me millions of email addresses. All of these are blatant lies, and most certainly a rip-off. Most Spam today only wants to get your email address validated. **So never, ever reply. Never!** They want to sell the names to other spammers, or poor suckers who actually think they can get rich sending unsolicited email.

These Ten Email Spam warning signs are the main things to watch out for!