Title:
Email Fight Club - Avoiding Spam, Spyware, Scams And Cookie Hunters

Word Count:
872

Summary:
Email Fight Club Rules

Follow these 10 common sense suggestions to avoid email trouble.

1. Suspect Everyone: Most unsolicited email is harmless junk from someone just hoping to make a sale or generate a list. However, there are some unscrupulous players out there (You know...the one with the rich uncle that just died in Nigeria) that are trying to scam you. Never reply to these unsolicited emails. Even "unsubscribe" will alert the senders that your email address is ...

Keywords:
spam, spyware, cookies, scams, self defense products, spy & surveillance equipment

Article Body:
Email Fight Club Rules

Follow these 10 common sense suggestions to avoid email trouble.

1. Suspect Everyone: Most unsolicited email is harmless junk from someone just hoping to make a sale or generate a list. However, there are some unscrupulous players out there (You know...the one with the rich uncle that just died in Nigeria) that are trying to scam you. Never reply to these unsolicited emails. Even "unsubscribe" will alert the senders that your email address is being used. If it looks to be of interest and they list a web site, type it into your browser to check it out.

2. "Just Say No" to Porn: Nancy Reagan was right! You know where the bad stuff comes from, so filter it out. Messaging software filtering tools will reject mail from your frequent spammers' email addresses, or with certain words ("sex", "porn", or "free meds", for example) in the subject line. It's easy to set up. Just log on to your email, click on "settings" and follow the directions. Even I could figure this one out without asking my wife for help!

3. Avoid SPAM - It's Nasty: Almost every Internet Service Provider has a spam

blocker these days. If yours doesn't (you should probably switch), there are several good third party spam blocking services such as Brightmail (http://www.brightmail.com). I have several email accounts, and for kicks I note how much email gets tossed into the spam folder every day. Typically, it averages around 2500 - 3000 per account. I run a couple of Internet businesses, so that number is quite a bit above average for a single user. I do however, thank the geeks that developed spam blocking every day.

4. Join Users Anonymous: Unless you are involved in Internet Commerce of some sort (and want as much exposure as possible), you should pull your listings from the large directory services. You probably never (knowingly) signed up in the first place, but chances are, your email address is included in some large data bases. Directories such as Bigfoot, Infospace, Switchboard, Yahoo People Search, and Who where are good about taking your listing down if you ask them to.

5. Scramble Your Eggs: Encrypt and digitally sign all your sensitive email messages. This is a bit of a pain, but you only need to get burnt once to know how important it is. If your messaging software doesn't support robust encryption, you can download PGP Freeware encryption software at http://web.mit.edu/network/pgp.html. Leave it up to the geeks at MIT (No offense intended Matt). Most messaging systems have industry standard encryption capability. If you are like me, you probably just never cared to notice.

6. Use Zip-Locks: Zip and Encrypt important attachments. Most modern computers come with WinZip installed. If you don't have it, you can find it at (http://www.winzip.com). Easy to use software that will compress and password protect your attachments.

7. Don't Eat the Cookies: Cookies are trackers that remember your IP address. They are convenient for sites that you use often and don't want to go through the entire validation process. However, some evil-doers will send you email with a sort of "cookie collector" to snag your info. Problem here is you might already be a goner before you realize it's a bogus email (especially if you neglect suggestion 3). To avoid cookies sent via email, use email client software, such as Eudora Pro, that lets you shut off its automatic Web Browser rendering engine. This step is a little hard core for the average Joe, but those of you who need it know who you are.

8. Mind Your Own Business: Avoid using your browser to read email on someone else's machine. If you are a busy body and insist on snooping, ALWAYS use "Clear History" when you finish to prevent subsequent users from getting into your mailbox.

9. Never get "Personal" at work: Violation of this simple rule gets more

people burned than any other act of defiance in the modern workplace. We had quite the network of great videos (You know the kind I mean) and jokes floating around the LAN on the last ship I sailed in...until one of the Server IT people showed me what they can spy on. Trust me--BIG BROTHER IS WATCHING! Never send sensitive personal messages on your work machine.

10. Let Norton Cook: This is just so basic that you probably SHOULD be burned if you blow this one. Keep your anti virus software updated. I know it sucks when it is time to pay again; especially when you haven't had a problem for two years...but paying for those routine updates is probably why you haven't. If your hard drive fried today, would you pay someone 30 bucks to make it all better right this instant? Thought so--Update it!

And the # 1 Rule of Fight Club is...

...........NEVER EVER under any circumstances EVER EVER leave your email logged on and your desk unoccupied at work! If you do, you have no one to blame but yourself. A co-worker's open email account is fair game--and it's "Take no Prisoners" time!

Well, that's it. A few basic do's and don'ts that will keep you in the fight and keep you out of trouble.