From the June 2009 Issue

I was originally planning on writing my column about a particular type of advertisement
I've seen online lately that I've found to be particularly annoying.
Specifically, I'm referring to one that says, "This is not a joke,
you're the 10,000th visitor!" while blinking incessantly. I am not
advocating the establishment of advertising content police, but when I see a
blatantly misleading ad like this on Yahoo!, Google and other reputable websites,
it makes me think such websites have abandoned some of their principles.

Quite obviously, Yahoo! has had more than 10,000 visitors (Yahoo! actually averages nearly 20 million visits per day). Perhaps it's a sign of the challenging economic times, but there are plenty of websites and other media outlets, like ours, whose advertisers are respectful to their potential customers.

Then I started thinking about abusive and even potentially threatening emails that we are subjected to every day. According to Microsoft, unsolicited email (spam) "accounts for more than 85 percent of all email sent each day."
This isn't really news, I guess. I am not talking about all commercial
email, which is, of course, a vital part of many legitimate marketing strategies.
And I'm not even talking about all unsolicited email, since most of it
is legitimate in messaging, content and intent. Instead, I'm referring
to the worst of the bad junk mail, the contents of which are often offensive
and promote a hoax or inciting illegal actions. Of course, anybody that has
used email for more than a month knows that these messages aren't worth
the paper they aren't written on. But it can be cumbersome to try to manage
and separate the good from the bad, the worthwhile from the trash.

For many recipients, the problem is compounded based on the length of time

abide by these rules because the penalties can be significant. But if you don't know who or what the company is that sent you the email, it very well could be from one of the mass spam abusers, who usually masks its true identity or uses "hijacked" computers to send the email. And they are often located in countries with little Internet regulation. If you try to use the unsubscribe feature on some of these messages, it may actually increase your likelihood of more spam because the action lets them know that they actually have a real and active email address.

But even these bad spam messages don't really pose a problem to most of us, aside from being an added nuisance. Especially since most are so horribly crafted that they expose their falseness. There are, of course, much more sinister varieties out there, from low-tech variations of old scams, to higher-tech missives that have the potential to actually do harm to your computer or extract personal sensitive data from it.

NIGERIAN SCAM & PHISHING

The oldest of them all is the low-tech Nigerian scam, which predates the Internet, but which has apparently thrived with the advent of email. Even so, it remains low-tech because they invariably ask the user to contact the sender in order to receive a cut of some multi-million dollar fortune for helping relocate it. As such, these scams pose little threat to honest persons or anybody with half a brain.

This original phishing model (phishing is the term for emails that try to get users to voluntarily disclose information), has been followed by uncountable variations, from still low-tech emails proclaiming the reader won some unknown lottery or promotion and one coming from a purported Iraq War veteran looking to move looted money from Iraq, to the slightly more tech-enabled bank scams

(I received three just today). In these, the email recipient is alerted to a

While you really shouldn't even open email from people you don't know, especially ones with obviously bogus subject lines, I admit that I occasionally read these emails (with images blocked). And what has always amazed me is that regardless of the variation on the scam, the creators of it are in dire need of English lessons. They might even be a little more successful if they'd get a copy of Rosetta Stone (www.rosettastone.com) or the Franklin Speaking Global Translator (www.franklin.com). I guess we don't really want that, though.

DON'T OPEN THIS

There are more nefarious, actively evil emails out there, of course. The more tech-capable villains out there develop various programs by which to attack unwitting recipients. These neo-Trojans send out email in the form of fake greeting cards, business proposals or other messages that include an attachment (often labeled as a video clip, PDF or Excel file) that, when clicked, will put a malicious program (malware) on the user's computer, which can be a virus, install a keylogger (which can steal your credit card numbers, passwords and other data), turn your computer into a spam sender, or pose other threats.

The most vulnerable to any of these threats are new computer users and often seniors, who are frequently targets of any type of scam. But none of us are immune, which is why smart email management and usage is an ongoing process. Creating customized spam folders that redirect any email with particular words (like the little blue pill and others) can provide some relief, and some people use white list tools that essentially only allow people they know to email them or include verification tools the first time a message from an unrecognized sender comes through. Other technologies are also available, including remote email filtering, such as that offered by AppRiver (www.appriver.com).

Personally, I just don't open attachments from people I don't

threats (PC World: "Malware Targets Macs" www.pcworld.com/article/163632). And it's not just email and computers anymore; the latest innovation in phishing is now hitting smartphones via smishing, a phishing scam sent via SMS messaging (texting). Viruses have also spread to social networking websites including Facebook and Bebo.

As tired of spam, viruses and other technological threats as everybody is, they probably will never go away, regardless of attempts at better laws like the CAN-SPAM Act. And there are two reasons for this: First, as P.T. Barnum said, "There's a sucker born every minute." In the Internet age, this equates to "There's a sucker clicking through every second." And secondly, as we get better at recognizing the threats, the bad guys will change their techniques, and maybe eventually take an English class.

- Here are a few simple no-brainers that I'm sure you know, but feel free to share them with someone who needs to hear this information (we all know a few).
- Your bank will never contact you by email about an "urgent matter." For people who receive their statement notifications by email, they won't/shouldn't include it as an attachment. Just go to their website and login.
- That email from somebody in Africa is bogus. Come on. Even if it were real, you'd be breaking federal laws by aiding in the scam.
- The IRS and Treasury will never contact you by email. If they owe you money, they'll either send you a check or send you a letter explaining the situation. After all, they have your address, not your email address. I've

found humor in these the last few years since they are written by the same

- Don't pass on emails that say "pass this on to everybody you know." Please stop.
- And finally… **You are not the 10,000th visitor.** You are not a winner.

Technology