

Enough nuisanceware!

Who wants to update contact info for a mere acquaintance or get a useless virus notice?

Sender: Out of the office

Recipient: Out of the office

Sender: Out of the office ...

By **DOUG BEDELL**
Technology Writer

It's bad enough that e-mail users must wade through endless batches of offensive spam, Nigerian financial scams and "phishing" attempts to steal their passwords and credit card numbers.

Now messages from well-intended software programs are causing confusion and frustration. Most notable are services such as Plaxo, AccuCard and PlanetID, which ask you to update your information in someone else's electronic address book.

Not far behind are messages from anti-virus programs that accuse you of sending virus-infected e-mail to some stranger. And then there's the e-mail loop, resulting in thousands of messages informing you that the other party is out of town or on vacation.

Here's a look at e-mail "nuisanceware" and suggestions for escaping the assaults.

Address book updates

Sample message: "I'm updating my address book. Would you please take a moment to re-

view your contact information? I keep my address book up to date using the XXXX service. Your updates will also help other service subscribers who already have your contact information."

The problem: Many people say the update requests feel like spam. And e-mail users don't know whether their information will be shared or sold if it is stored on a third party's server.

Considerations: These update programs are used by people who have your name in an Outlook, Outlook Express or Web-based address book. The contact lists are stored on the updating service's computer, which can be instructed to send out e-mail asking that you confirm your information.

Each of these update services says it will keep your information private and not allow it to be spammed. Wary consumers, however, remember what happened to databases during the dot-com bust. Many privacy policies were voided when firms gobbled up each other or filed for bankruptcy.

Plaxo, with 2.1 million users probably the largest service, says subscribers will be allowed to delete their address book information if the company changes

hands or fails. But if your contact information is in someone else's address book, you can't get rid of it.

"We don't allow anyone to see your address book," says Rikk Carey, Plaxo vice president of engineering. "And we don't allow anyone to delete it, either."

Many PR executives, salespeople and others with extensive business contacts rely heavily on these contact updaters. They also provide invaluable backups for their databases.

Solutions: "This to me is just a lazy way of updating a Rolodex," says Jana High, Southern Methodist University adjunct professor and author of *High-Tech Etiquette* (Rawdon & Watson, \$20). "My best advice is to e-mail back to the person. Tell them that, unfortunately, you don't have the time to provide that information."

If the person is offended, Ms. High says, promise to send them the information on a business card via snail mail.

Many services let you opt out of update requests from indi-



duals or servicewide. But getting out still requires that you take action on a message you never opted in to receive.

If you don't know the person by name, chances are it is best just to delete the update request and forget about it.

You're infected!

Sample message: Attention! Content violation! The Rio Linda Union School District's anti-virus gateway found the content in a message sent by this account violates anti-virus gateway policies. The message and/or the attachment have been deleted. Please take appropriate actions. Thank you.

The problem: You never sent any message from that address to the Rio Linda Union School District. In fact, you don't even know where Rio Linda is.

Considerations: Symantec and other e-mail virus/worm scanning software makers developed these auto notification features before the advent of mass-mailing worms. Worms routinely use other people's e-mail

addresses to send out their payloads.

Most system administrators who have updated their anti-virus programs simply delete infected messages and don't send courtesy e-mail because it's unlikely the sender is at fault.

Solutions: Calls to your service provider's help desk aren't necessary when you receive messages about infections that are obviously not your fault.

If the recipient is someone in your address book, you should double-check that your computer is clear of macro viruses. Free virus scans are available online from numerous Web sites, including McAfee.com, Trend Micro (housecall.trendmicro.com) and PandaSoftware.com.

If you know that you're getting notifications as a result of a mass-mailing worm's activity, try writing administrators at the network that sent you the alert.

Out-of-office loops

Sample message: "I am out of the office and will answer your e-mail when I return."

The problem: Autoresponders can generate thousands of unnecessary e-mails when they attempt to answer each other. This looping often occurs when spam or a virus hijacks your e-mail address and sends a message fielded by an autoresponder. If your address is in a group, everybody gets a copy. And if someone in the group has turned on an autoresponder, e-mail servers can wind up sending each other thousands of vacation messages, and you get a copy of each one.

Considerations: Many experts urge users to stay away from autoresponders, period.

Solutions: Every e-mail server on the Internet is supposed to have an active address in the form postmaster@thedomain.com. Any postmaster who allows autoresponse looping to occur deserves a nasty e-mail from victims. You can complain and you can filter your incoming mail. But those are about your only options.

E-mail dbedell@dallasnews.com

