Out Behind the Barn
Dans le feu de l'action

Email — from friend or foe?

Barry McCombs, MD, FCFP
Medical Information Service Coordinator, Alberta Rural Physician Action Plan, Calgary, Alta.

Correspondence to:
Dr. Barrie McCombs,
3111 Utah Dr. NW,
Calgary AB T2N 3Z9;
barrie.mccombs@rpap.ab.ca;
www.vlibrary.ab.ca

Despite the efforts of software companies and computer users, those sleazy folks who send out junk mail keep finding new ways to creep into our email inboxes. This article describes some of their current tricks and ways to minimize your risk.

CASE 1

For awhile, I was frequently receiving "advertising" messages from another physician's email address. She didn't send them and her other contacts reported the same issue. The problem persisted despite updates to her security software. Her computer had likely been infected with an undetected virus-like program that was sending junk mail to everyone in her email address book. Since the messages came from a personal computer, they were not identified as spam by my email security programs.

CASE 2

While investigating the first case, I learned from my system supervisor that some virus-like programs send email messages from one contact in an infected computer to another contact in the same address list. This makes it even more difficult to identify the real source of the problem.

CASE 3

I've also received fraudulent messages, supposedly from known physicians, asking me to become their "friend" in a social network website (such as Facebook). This trick is apparently used by companies that sell email address lists. If you agree, they install a virus-like program that reads the email address book on your computer. I never reply to these messages directly, but do send a separate message to the physician to advise them that their computer may be infected.

PRACTICAL PARANOIA

To avoid virus infections, be suspicious of all incoming messages, even from friends. If available, use the "preview" feature of your email program to read messages without actually opening them. This reduces (but does not completely eliminate) your risk.

ADDRESS FIELDS

The address fields (From, To, CC) of your messages can give warnings. If a message was sent to several people, your risk may be greater. Messages from legitimate sources may be flagged as spam if sent to multiple recipients using the BCC (blind carbon copy) field, which is never displayed to the recipient. Some recent spam messages have been sent from a fictitious "Doctor Smith," just to make them look more important. Putting blocks on messages from a given address is rarely effective, since the junk mail senders change the sending address frequently.

SUBJECT FIELD

Blank or vague subject fields may be clues to unwanted messages, but are often due to human error by the sender. Security programs may add a flag to the subject if they detect possible spam or fraudulent messages. Your email program may allow you to flag messages

as spam if they contain certain recurrent words such as "Viagra" or "male enhancement."

MESSAGE TEXT

Most email users learn to recognize common junk mail themes, such as "get rich quick" schemes or dire warnings that their credit cards or bank accounts have security problems. Financial institutions are unlikely to use email to tell you about such problems.

MESSAGE LINKS

Don't click on links in suspicious messages, even from friends. This is a common way for viruses to spread. It is safer to retype (or cut and paste) the address into your Internet browser program if you wish to visit the website mentioned. Security programs scan links to determine if the link matches the message text. This unfortunately can result in some legitimate messages being flagged as fraudulent.

ATTACHMENTS

Attachments are also a virus risk, particularly if they contain executable code, such as Microsoft Word or Excel files. Be suspicious about unexplained attachments in any message. While we're discussing attachments, you can avoid overloading your email inbox by saving large attachments (e.g., photographs) to your hard drive and then deleting the message.

REPLIES

Don't ever reply to junk email messages. That just confirms that your email address is still active. Unless you really trust the sender, never use message links that claim to remove you from the sender's mailing list. If you receive a suspicious message from a friend, ask them to confirm that they actually did send it.

UPDATE YOUR SOFTWARE

Make sure that both your computer operating system and security programs are automatically sending you updates whenever new threats are detected. As an extra precaution, visit the vendor's website occasionally to confirm that your software is current. One of the concerns about the recent "Conficker" virus was that it was designed to interfere with receiving such updates.

Competing interests: None declared.