

**Computer Troubleshooters
Henderson**
P.O. Box 83-104
Edmonton

mark@ctshenderson.co.nz
www.ctshenderson.co.nz

T: 835-0479
F: 836-2345

Offices Worldwide

Australia, Austria, Bulgaria,
Botswana, Canada,
Democratic Republic of the
Congo, Egypt, Ghana,
Greece, Guatemala, Hong
Kong, India, Kenya, Kuwait,
Malaysia, Mexico,
Netherlands, New Zealand,
Nigeria, Portugal, Republic of
Ireland, Romania, Singapore,
South Africa, Spain, United
Kingdom, United States of
America

International Website

www.comptroub.com

Computer Troubleshooters
The World's #1 computer
service franchise network

Global Newsletter December 2008



Holiday Greeting or Virus?

If an email arrives in your inbox, claiming to be an electronic greeting card from a friend or family member, would you automatically open it? New research by global internet security company AVG Technologies found that 74 per cent of the people polled said they would automatically open the email.

Criminals misuse our trust in familiar names. They send their security threats with false 'from' addresses to get us to think the information has come from a trusted source. Reputable companies are also not immune, with one reported case of emails being sent in the name of the Deputy Director of the USA's FBI department.

If your computer is up to date with functioning security software, do you need to be concerned? Well, just like you need good driving skills in a car that has many safety features, good email habits can also help to protect your precious information. Sneaky attacks like identity information gathering (known as 'phishing') can also be difficult to detect.

Remember these tips for the next greeting card that arrives in your inbox:

- 1. Check the spelling:** Look out for misspelled words, names or website addresses, which are a good sign that the email is not genuine.
- 2. Read the fine print:** Carefully read any terms and conditions that you have to accept before viewing your card, especially if the card site wants to install any software onto your computer. You may actually be agreeing that the site can have access to the details of everyone in your address book.
- 3. Don't open attachments:** Save any attachments and scan them with your security software before opening them.
- 4. Avoid clicking on links:** Links to websites may look legitimate, but they can hide malicious code that activates once the link is clicked. Instead, most e-card companies allow you to visit their website by typing the site name manually into your web browser and then entering a code to retrieve your card.
- 5. Phone a friend:** If in doubt, delete the email or call the sender to confirm that they really sent it.

Talk to your local Computer Troubleshooter if you are concerned about the contents of an e-card that you have received.

OVER
450
LOCATIONS WORLDWIDE




**Contact your local Computer
Troubleshooters**

Mark Argent
835-0479