



LG Electronics Canada Inc.
550 Matheson Blvd East
Mississauga, ON L4Z 4G3

August 29, 2007

Email Hoax:

LG Electronics has learned of several emails being sent to the public which falsely claim that the recipient of the email has either won a sweepstake or been randomly selected for a cash prize from our company. The emails often contain a qualification or other type of claim number as well as a person to contact, typically an "Executive Secretary". Sometimes the email requests that recipient send personal contact or other identifying information to a provided contact person.

We have observed a number of versions of this scam. One is purportedly run in conjunction with United Nations Organization and European Union and the recipient is told he or she is one of 50 worldwide recipients of a cash award of \$2 million to be used for the business, education or personal development of the recipient, with at least 30% to be used for environmental development. Other versions claim that the recipient is the winner of the LG National Lotto/International Promotions or similar program lottery. Samples of the various versions of this email scam that have been recently circulated are included below.

View samples of email hoaxes we have identified. NOTE – Samples included via this link contain a representative sample of email hoaxes in circulation that have come to the attention of LG Electronics. Other email hoaxes may exist and may not be included here.

Our Response:

Please be advised that these emails are hoaxes and neither LG Electronics nor any of its affiliates are sponsors of or in any other way associated with these emails or programs. The LG names and trademarks are being used without permission and we are currently in the process of investigating this matter.

This email appears to be a form of fraud commonly known as "phishing", the objective of which is to try to obtain personal or financial information from you.

How to tell if an e-mail message is fraudulent:

Here are a few warning signs that the message you received is a "phishing" scam:

- **You are asked to provide personal or financial information** - Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.
- **Message conveys a sense of urgency** – "Phishing" messages attempt to convey a sense of urgency so that you'll respond immediately without thinking.
- **Bulk emails** - Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.
- **Spelling and grammatical errors in the email.**
- **Sender's use of free, non-corporate email accounts (such as Yahoo!, AOL and Hotmail).**

What to do:

Please do not respond to these emails, as it could jeopardize your personal information and privacy. If you have already responded, we advise that you immediately discontinue all communications with any of the individuals associated with this hoax. You might also want to report this email to the Competition Bureau at Industry Canada at 1-800-348-5358, to the Royal Canadian Mounted Police at 1-888-495-8501, as well as to the Anti-Phishing Working Group at reportphishing@antiphishing.org.

In addition, you may want to consider using anti-phishing/anti-spam software to protect yourself against this type of fraud. Many internet service providers offer this type of software as part of their customer service offering. Alternatively, you may choose to independently purchase anti-spam software which is readily available wherever software is sold.