

Anti-Spam Legislation

We've put together some helpful information from the Unsolicited Electronic Messages Act 2007 to assist you in understanding what is considered spam and how not to be a spammer.

Summary

As of 5 September, the Unsolicited Electronic Messages Act 2007 comes into effect. The purpose of the Act is to deter people from using information and technology communications inappropriately and encourage good direct marketing practice. It is geared to decrease spam in New Zealand, which the Act identifies as electronic, commercial and unsolicited messages (including e-mail, text & instant messaging). In addition the Act lays out rules for sending commercial electronic messages: mainly that you must gain consent, identify who you are and include an unsubscribe link (you have 5 days to remove following a request). However, the Act is not applicable to common messages between organisations and their clients/customers such as factual information about a subscription, membership, account, loan or similar ongoing relationship. The process for obstruction by a person/company is that they would receive a formal warning, followed by an infringement notice (up to \$2,000 per infringement) and lastly court actions (up to \$500,000). Internal Affairs will be policing the Act and stated in a recent seminar that the legislation as a whole is more of a "may vs. a must" of what Internal Affairs can do to offenders. For more information please visit the Internal Affairs website.

What is spam?

Spam is the generic term for the electronic commercial "junk mail" you receive without having requested it. This includes unwanted messages sent to people"s email accounts or mobile phones. Current estimates suggest that around 12 billion spam messages are sent every day. These emails clog the Internet, disrupt email delivery, reduce business productivity, raise Internet access fees, irritate recipients and erode people"s confidence in using email. These messages are essentially commercial in nature and often sent in bulk. Some spam is sent by legitimate businesses inviting the recipient to buy a product or service. Other spam may attempt to trick people into divulging their bank account or credit card details. While some spam messages also contain offensive or fraudulent material and/or spread computer viruses.

How do I know if my message is spam?

Your message might be considered spam if it is:

- Electronic: emails, instant messages, SMS multimedia message services and other mobile phone messages
- Commercial: marketing or promoting goods, services or land, or directing the recipient to a commercial location such as a website
- Unsolicited: when recipient has not consented to receive mail

What spam is not

The act takes a common-sense approach and excludes a range of common communications between businesses and their customers including:

- Responses to a request for a quote or estimate
- Messages that facilitate, complete or confirm a commercial transaction that the recipient previously agreed to
- Warranty information, product recalls and safety and security information about goods or services used or purchased by the recipient
- Factual information about a subscription, membership account, loan or similar ongoing relationship
- Information directly related to employment or a related benefit plan which the recipient is currently involved
- Delivers goods and services that the recipient is entitled to receive under the terms of a previous transaction

How to not be a spammer

Internal Affairs has specified three requirements to ensure that you're not considered a spammer.

1. Gain consent of the addresses you're sending email to. This can be obtained expressly, inferred or deemed.
2. Clearly identify yourself as the sender and how you can be contacted.
3. Include an unsubscribe link such as "If you do not wish to receive future messages, send a reply with UNSUBSCRIBE in the subject line."

Reducing spam

The Unsolicited Electronic Messages Act 2007 will enable Internal Affairs to fight NZ sourced spam and enter into international agreements concerning international enforcement of anti-spam legislation, sharing of information between national enforcement agencies and the pursuit of cross-border complaints. The Act seeks to support the use of email for legitimate marketing purposes where the interests of the recipient are duly respected, but prohibits spam with a NZ link and the use of harvested addresses.

Known spam scams

Nigerian scam

From: frank victor
sonofgovernor@yahoo.com

i am frank, son of governor of lagos state of nig. i am looking for any bank manager over there tocontact i want to have savice acconut over there i am coming over there soon to stay and invest my money be fore then i need a bank manager that i can have his acconut number let me transfer all my money to him…so bye and god bless you from fr.son

The Nigerian spam

explained: A respondent is told that they will receive a generous commission to help transfer millions out of the country. But first stamp duty or bribes must be paid. A small investment on the promise of a large return. But the demands for more money never stop. By the time the respondent figures out they have been conned, they have paid over hundreds, if not thousand of their own money.

Russian Bride

Subject: Hello I need love and dating!!!

Greetings, Good Hello my friend!!!! You probably do not know who I and what for I have written to you the letter. I am Elena from contry Russia…I would like to know you want to get acquainted with me whether or not? I search the man for love and more even =for a marriage…So I wait for your answer…Your new the girlfriend from Russia Elena!!!

The Russian Bride Scam

explained: This is a variation on the Nigerian scam. The young woman would like to meet you but needs money for a passport and airline tickets. Once the money is sent the email account closes and the love-struck man is left poorer and feeling foolish. The alternative is just email me back and I will get a refund from the agency that selected you!

Something's ‘Phishy’

Dear eBay Community: We have decided to close eBay on 27 February 2007 due to the repeatedly abuses on our company. We ask your opinion on this matter…If you want eBay to stay open click YES otherwise click NO. Your opinion is very important to us. If 50% of the eBay members vote positive eBay stays open otherwise it will be closed. Regards, eBay Team

The phishing spam explained: Ever received an email from a bank that you're not a customer of, asking you to confirm your account details? Phishing is the act of tricking someone into giving them confidential information, or tricking them into doing something that they normally wouldn't do or shouldn't do. This is a classic example of a phishing attack where the hook is a poll based on eBay being closed because of so many phishing attacks?

Fast Track

Genuine Qualifications: A Genuine University Degree in 4-6 weeks! Have you ever thought that the only thing stopping you from a great job and better pay was a few letters behind you name? Well now you can get them! BA BSc MA MSc MBA PhD Within – 46 weeks! No Study Required! 100% Verifiable!

Fast tracked qualifications explained: Basically this is a misrepresented or worthless product.

Viruses

The scooby snack teaches the tornado. Any lover can share a show with the cloud formation inside the tomato, but it takes a real recliner to bury the moldy globule.

Explained: Some spammers use machine generated language to either get around the filters by using non-standard spellings and orderings of words. While these emails will generally be your VIAGra type emails requiring you to click on a link to go to a website, OR they can be used to harvest addresses for future spam attacks. They can also contain viruses, trojans, malware and spyware.

How to protect yourself from spam

In today's E-society we necessarily depend on electronic communication to conduct business, exchange information, and simply be social. So how do you protect yourself and others from spam?

-

Limit the amount of non-essential emails you send, particularly mass forward stories or jokes.

-

Ensure your anti-virus software is up to date, as well as installing and running anti-spyware.

-

Never
click on the REMOVE link unless you can verify the sender, as this will
validate your email address and be sold to more spammers.

-

Report spam by sending the message plus the full header to spamcop.net or abuse.net.

-

Use
unusual email addresses containing numbers and letters i.e.
dan231@yourdomain.com to avoid spammers who use computer programs to
guess email addresses.

-

If you have a website, provide a form for people to contact you and ensure that the "send to" email address is not contained in the HTML, but in the form processing script.

-

Avoid anti-spam software that bounces spam emails, as the bounce message will go to an innocent person, possibly turning you into a spammer.

Useful websites

www.stopspam.org.nz

www.antispam.govt.nz