



Minicorp Newsletter

www.minicorp.com.au

Issue 001 | 16th March 2010

We'll be sending you tips and ideas for your small business, and keeping you up-to-date on business related information and concerns.

In This Issue:

- > Welcome To Our First Newsletter Issue
- > Spam Email ~ Phishing Scams

Minicorp:

- > About Us
- > Our Services
- > Areas We Service
- > Our Work Examples
- > Contact Us

Minicorp
14 Alpine Way
Kilsyth VIC 3137
(03) 9728 5038
0433 376 389
www.minicorp.com.au
ABN: 55 686 954 079

If you no longer wish to receive this newsletter or any future marketing material from Minicorp, you can unsubscribe here.

Welcome to Our First Newsletter Issue

Hello, and welcome to our first Minicorp Newsletter. We'll be sending you information on tips and ideas for your small business, and keeping you up-to-date on business related information and concerns. We hope you find the information helpful and informative.

~ Remember to call Minicorp for all your small business needs ~

Spam Email ~ Phishing Scams

There are currently these types of emails in circulation



Email and the Internet is a wonderful resource that has revolutionised the way humans communicate and access information. Unfortunately, it has also proved to be a fertile medium for the unscrupulous and the morally challenged. Scammers regularly use email in attempts to steal money or personal information from unsuspecting victims. Those inexperienced in the ways of the Internet are especially vulnerable to current Internet scams. The good news is that it is not difficult to learn how to recognise current Internet scams that arrive via email.

One type of email you may receive, is from a bank/online service provider/financial institution that asks you to click a link and visit a website in order to provide personal information. Such an email is more than likely the type of Internet scam known as "phishing".

A phishing scam is one in which victims are tricked into providing personal information such as account numbers and passwords to what they believe to be a legitimate company or organisation. In order to carry out this trick, the scammers often create a "look-a-like" website that is designed to resemble the target company's official website. Typically, emails are used as "bait" in order to get the potential victim to visit the bogus website. Be wary of any email that asks you to click on a link and provide sensitive personal information such as banking details. Information submitted on these bogus websites is harvested by the scammers and may then be used to steal funds from the user's accounts and/or steal the victim's identity.

Most legitimate companies would not request sensitive information from customers via email. **DO NOT** click on the links in these emails. **DO NOT** provide any information about yourself. If you have any doubts at all about the veracity of an email, contact the company directly.

Other hoax email types:

- Nigerian Scams
- Lottery Scams