# Cyber Crime

**The internet, it's a great place to play, shop, and communicate. However, it has also become the place for the "new crime" - internet fraud!**

Internet Fraud is increasing rapidly. After four days away from his computer, Steve's Junk Email box had dozens of emails from various dubious folk – all trying to extract money, data, or information from him. The levels of sophistication in their attempts are scarily good. They all target our human vulnerability and trusting nature.

The following are some of the more common attempts:

1. **Upfront Money - "Nigerian" Letter**


This is a low-tech, mass email approach. These letters are no longer just from Nigeria, they appear to come from all over the world. They attempt to sound credible by referring to important people or roles (e.g. "Chief Auditor of Lloyds", "Vice-President", "Managing Partner" etc). We are always amazed how many times somebody on the other side of the world wants to give us US$10.0m just because we seem to be nice guys. All we need to do is reply or click on a link to release this large windfall.

2. **Won-a-Prize**

Again, a low-tech, mass email approach. In recent weeks, we have won hundreds of thousands of dollars from "Google Incorporated" or "Microsoft Org" with such ridiculous claims as our email addresses were drawn from a hat. What do they want? The same as the "Nigerian' letter. They want our "click" to steal our personal stuff, get access to our bank accounts or even take-over our computers using sneaky bots, viruses, or bugs.

3. **Invoice for Payment**

- Low-tech, mass email invoice – e.g. Origin Energy email received confirming power usage and getting us to pay online by clicking on a button or link. The invoice even looked genuine with a logo etc. However, we don't have an Origin Energy account, and even if we did, any payment made by clicking a link certainly wouldn't be going to them.

- High-tech, targeted invoice. This is more difficult to detect as they steal an existing invoice from a major supplier, eg. Placemakers, and send fictitious invoices out to known building contractors with one key change - the bank account number. These invoices look genuine and, in many cases will match building jobs currently in progress.


4. **Bank or IRD – Update your Details**

Every day we receive emails purportedly from Inland Revenue, KiwiBank, ANZ, BNZ, or other banks telling us that we need to "click" on the link to update our bank account log-in details. These emails look scarily good, complete with bank logos. They want you to "click" on the link they provide. This will take you to a false, but very authentic looking websites, where you will be asked to put in your password, and to then change your details. The fraudsters now have your bank log-in details and password and can now access your account.

**5. Investment Scams**

A scammer calls or emails claiming to be a share broker or portfolio manager and offers financial or investment advice. They will claim what they are offering is low-risk and will provide you with quick and high returns, or encourage you to invest in overseas companies. These are backed up by genuine looking paperwork and a clone website with slick, high-pressure sales tactics and repeated calls / emails.

There is no such thing as a 'free lunch'. Even if these fraudsters did have an investment to promote, it would not be low risk. You'd be safer putting money on the roulette wheel!


## 8 Tips to avoid becoming another victim?

1. If something seems too good to be true, it probably is! Be alert for anything suspicious in emails including poor grammar and punctuation.

2. If in doubt, don't reply to an email or click on a link. To check where an email is really coming from, hover your mouse over the link or the name of the sender. If you don't know the person or the address is not identical to the company's website or email address then delete the email and block the sender.

3. Your bank or Inland Revenue will never send you a link to click on. If they want you to do something, they would ask you to go to the website and log-in in your normal fashion.

4. Ensure your computer software and anti-virus is up to date.

5. Have good passwords with combinations of upper and lower case, numbers and symbols. Change your important passwords regularly.

6. If an organisation asks you to change the bank account number before paying a bill, ring the company to check it is a legitimate change and the new bank account is correct, remembering to use the contact details from an old invoice (not the suspicious one).

7. Arrange for all regular bills to be paid by direct debit, therefore reducing the chance that these invoice scams could work. Never use a link to pay a bill.

8. Don't be swayed by unsolicited offers promising bargain deals or instant riches, or be pressured into making a decision. Legitimate companies give you time to do research and think about it. Don't try to engage and feel free to hang-up on calls or delete unwanted emails.

While the internet is a wonderful thing, it does come with its pitfalls. It presents fraudsters with a way of stealing your money, information or identity. We must therefore be aware of the risks and warn others – which is what we are doing now!

For more information, we recommend you visit www.netsafe.org.nz, a NZ organisation focussed on online safety.