



## Internet scams

### The Set-Up

The internet is an exciting new frontier, where anonymity still reigns.

### The Hook

The internet has brought amazing new possibilities right into your home.

### The Sting

The internet has also brought with it a whole new tide of scams and untraceable scammers.

## What an internet scam looks like

The internet is full of scams. You might not even notice you have been stung until your credit card statement or phone bill arrives.

Scammers use the anonymity of the internet to rip bidders and buyers off. You could end up with a dud product or nothing at all ... or with your bank account or credit card details in the scammer's hands.

## Variations of internet scams

### Spam offers and internet junk mail

These usually offer free goods or prizes; very cheap products, including pharmacy drugs; cheap travel, psychic advice, fake college degrees, counterfeit watches, financial promises and other offers that sound attractive and more-or-less legitimate.

In some way, all these scams will try to get money or personal details from you, such as:

- a joining fee
- a purchase
- a qualifying purchase for a prize or
- a call to a high charging premium rate (0900 or overseas) phone or fax number.

Spam junk mail is much more dangerous than junk mail through your letterbox, because if you click on the link it can launch spyware that monitors your computer or even a keylogger, which is a programme that sends the scammer a record of everything you type, including your bank passwords.

The Unsolicited Electronic Messages Act 2007, which came into effect in September 2007, aims to prohibit spam sent to, from or within New Zealand. It is expected that this law will reduce the amount of spam that New Zealanders are targeted with. To find out more, go to the anitspam section of the Department of Internal Affairs.

[Visit the Department of Internal Affairs website.](#)

### Free offer scams

They can come to you as spam emails or appear as annoying pop-up windows, banners or even entire websites. They offer free access to restricted sites, free shares, downloads, product trials or even holidays. But to claim your free stuff you need to provide your credit card or bank account details. Then they have you.

### Online auction scams

Because most auction sites have anti-scam measures in place, most scammers will try to get you to go outside the auction process to do the deal. For instance, they may contact you to say the winner of an auction pulled out: would you like to buy the product instead, privately? You may never see your money again.

Another trick is auction rigging. If you are selling: a scammer can put in a low bid, then a very high bid under another name. Just before the end of the auction, they will withdraw the high bid, so that their low bid wins. If you are buying: the scammers may use false bids to get you to bid higher.

## Social networking sites

Someone phishes your log-in details and hacks into your social networking site - assuming your online identity. Suddenly, your social networking friends are deluged with spam, links to dodgy websites or requests for you to wire money to them.

One report to Scamwatch said: "I received calls from two friends in Australia saying that they had been 'chatting' to me on Facebook. Apparently I was in London, had been robbed and had lost everything. I then asked these friends to "loan" me \$700 to be sent immediately via money transfer. My friends had the sense to ring me in NZ to check to see if the story was correct. Obviously it wasn't..."

## Miracle cure scams

When the product doesn't arrive, or does arrive and doesn't work, the anonymity of the internet can make it very hard to get your money back.

## Cheque overpayment scams

A scammer sends you a cheque, but they have paid too much. They ask for a refund of the difference, which they hope you will pay before discovering that their cheque is worthless.

## Domain name renewal scams

If you receive a renewal request for your internet domain name, check carefully that it is coming from the correct registration authority. Scammers may also try to dupe you by charging you for a domain name that is very close to yours: they hope you won't notice and pay their invoice.

## Spyware and keystroke-loggers

As scary as it sounds, scammers have software programmes that can enter your computer, monitor what you are doing and even take various forms of control over your machine. For instance, a 'keystroke-logger' is an item of software that records every key stroke you make. So if you visit your internet banking and type in your password, the scammer can see what you typed.

Malicious software like this gets into your machine through hidden programs that may be activated when you click on links in spam emails or download certain files from the internet. These files are called 'trojans' because, like the Trojan Horse, they seem innocent on the outside - e-greeting cards, music or video files, for instance - but the dangerous stuff is hidden inside.

## Modem jacking

Not so much of an issue now most people are on broadband, but for dial-up internet, without your knowledge, your computer settings may have been changed to dial an expensive number every time your modem dials in to the internet. The result will be huge phone bills. The computer program that does this may have installed in your computer via spyware or a virus, or disguised as software that gives you access to restricted websites. These scams are decreasing as more people move away from dial-up modems to broadband, but if you have a dial-up modem, regularly check your phone bill for unusually expensive calls, and check 'Modem Properties' to see what number it is actually dialling.

## Protect yourself from internet scams

- Never open unsolicited emails (spam). Don't reply or click on links, even to tell them to stop. The only exception to this rule is when an unsolicited email is from a trusted, New Zealand source. The Unsolicited Electronic Messages Act 2007 requires all unsolicited emails originating in New Zealand to have a genuine 'unsubscribe' facility. In these cases, clicking on the 'unsubscribe' option will stop further emails of this nature from this source. However, if in doubt, it is better to be cautious and ignore the email. Never call a phone number listed in an unsolicited email. If in doubt, delete the email.
- The same goes for clicking on website pop-up boxes and banners at sites you do not trust. Don't click, just close.
- If a junk email contains an offer you just cannot resist, don't click on it but use the internet to check whether the company is a legitimate business.
- Always read terms and conditions attached to any offer. Look for hidden costs and obligations. Don't trust offers that don't allow you to read the terms and conditions.
- Do not enter your personal details, including credit card and bank account information, on any website you are not certain is genuine.
- Be careful: scammers can create websites that look just like a genuine website (ie such as a banks' website).
- Be wary of very low prices for products offered for sale. On that note, watch out for low-priced items that may have hidden costs, such as grossly overpriced shipping or handling fees. Read the terms and conditions carefully to spot any hidden costs.
- Don't send money to cover fees for unexpected prizes or mystery lotteries. You cannot win a lottery you have not entered. Lotteries like that don't exist.
- Before you take advantage of a free offer, check it out with other internet users you trust, or do research into the company making the offer.

- Be suspicious of any seller or shopping site that does not give their full contact details. A post office box is not enough to trace a scammer, especially overseas.
- Be careful of shopping websites that give poor privacy guarantees, terms and conditions, contact details and dispute resolution.
- Sellers: don't send refunds until you have confirmed the buyer's original cheque has cleared. Don't fall for a cheque overpayment scam.
- Consider using an 'escrow' service when you buy something over the internet. This means you can pay for your goods and your money is held by the service, but the money will only be released to the trader when you confirm you have received your item.
- Install internet security software, including virus-and-spyware checkers, and keep it up to date. The makers of this security software regularly publish updates to deal with the latest risks. Keep this software up to date.
- Be wary of internet websites offering free games, music or video. The files they provide could be trojans. There are many reputable websites offering free entertainment or resources to enjoy, so keep yourself safe by keeping your internet security software up to date.

### **Internet auction sites**

- Take into account the ratings given to buyers and sellers on internet auction sites.
- Resist suggestions to go outside the auction process to complete the sale.
- Be wary of sellers who demand immediate payment, or payment that gives you no way to retract or cancel, such as electronic funds transfer or a wire service.

### **Help protect others from internet scams**

If you have been the target of any kind of internet-based scam, please share your story here. We will treat your report in the strictest confidence and remove your personal details before posting your story on our site.

[Report your scam story to us.](#)