

## Email spam and scams



Australian  
Competition &  
Consumer  
Commission

### How do I find out more?

To find out more, contact the ACCC infocentre by:

**Phone:** 1300 302 502

**Email:** [infocentre@accg.gov.au](mailto:infocentre@accg.gov.au)  
or visit the ACCC website at [www.accc.gov.au](http://www.accc.gov.au).

Anyone who uses email in their daily business has no doubt come across spam mail—unsolicited commercial messages urging you to purchase a range of questionable products, including non-prescribed medication, counterfeit university accreditation or even vast fortunes of the Nigerian Royal Family!

At first glance, it might seem that these scams are relatively pointless—after all, how could anyone fall for them?

Unfortunately, research from the Australian Consumer Fraud Taskforce shows that an increasing number of Australians are falling victim to these scams in record numbers.

So how can you protect yourself? Fortunately, there are some simple rules you can follow to protect yourself—and your money!

### 1. If it seems too good to be true - IT PROBABLY IS

Scams almost always make

some kind of outrageous deal—send me \$500 and you will make \$50,000!

It is important that you remain sceptical when weighing up any offer—in fact, the best defence against scams is to just ignore any uncollected commercial offers. They are more than likely to be scams.

### 2. Don't be a vulnerable target

The most important thing to remember is that scammers are hoping to prey on a weakness of their target—greed, insecurity, loneliness, etc.

The best way to fight scammers is to not give them a target to begin with.

### 3. Check all web addresses carefully

One of the most common kind of scams targets your internet banking—you receive an email purporting to be from your bank, asking you to click on the enclosed link and update your security details.

However, the page you go to will not be that of your bank—it may look similar, or have a similar

name, but it will be one set up by the scammer to capture your login and password, giving them full access to your bank account!

The best way to combat this is to always enter the web address for your online bank manually—never follow a link in your email, no matter how 'authentic' it appears to be.

### 4. Never pay for unrequested goods and services

Another type of 'old' scam which has evolved into an internet scam happens when a business requests payment from you for unsolicited goods or services.

Generally, the invoice you receive will be for goods you never ordered, and never received!

Other times, it will be for goods you ordinarily use—such as printer toner or paper—from a company whose name seems *similar* to your regular supplier.

This scam relies on the fact that small business operators are always busy; the scammer hopes you will pay the invoice

without closer inspection.

The best way to combat this scam is to ensure that there is one person in your business who is responsible for all ordering and payments, and making sure that they double-check all invoices to ensure that goods were both ordered and received.

### More Information.

The *Scamwatch* website, [www.scamwatch.gov.au](http://www.scamwatch.gov.au) lists the most common scams in operation, including internet scams, and teaches you some common-sense techniques to protect yourself.

For more information, call the ACCC Infocentre on 1300 302 502 or visit our website at

### Did you know?

The ACCC publication *The Little Black Book of Scams*, is available free of charge by calling the ACCC Infocentre on **1300 302 502**.