February 2005

ACCC InfoLink

Scams Awareness Month
Small Business

How do I find out more?

To find out more, contact the ACCC infocentre by:

Phone: 1300 302 502
Email:infocentre@accc.gov.au
or visit the ACCC website at www.accc.gov.au.

In coordination with International Consumer Fraud Prevention Month, February is national Scams Awareness Month at the ACCC. Complementing the existing programs to inform and protect consumers (including business consumers) about frauds and scams commonly targeted against them, this month the ACCC will launch some special initiatives, such as Internet Sweep Day and new publications.

Scams

Small business owners and operators are usually very busy, and often do not keep track of all the government agencies, suppliers and customers they deal with.

Small businesses often get demands for payment for magazine advertising or entries in business directories that were never ordered or approved. On closer examination, some of these are merely offers to book a listing or an ad but are cleverly disguised to look like an invoice.

A similar scam you may come across involves an invoice arriving for common office supplies which you did not order. It may be an invoice for printer toner, fax paper or printer supplies from a supplier with a similar name to the company you actually use, with the perpetrators hoping that you will pay it without checking closely.

All these scams rely on you and your staff being busy and not thoroughly investigating every invoice which passes through your office. Scammers thrive on their victims' uncertainty and lack of organisation. Keeping accurate records and insisting on written confirmation of transactions will not only minimise your chances of being scammed, but also makes good business sense.

Online scams

The internet can be a cheap and efficient way to advertise and sell your products, keep in contact with your customers and suppliers, and even makes simple tasks like banking or paying bills quick and efficient. However, unscrupulous people may try to take advantage of the relative complexity and anonymity that the internet provides.

Many of the online scams which are targeted at small businesses are identical to those targeting consumers. Bank account fraud (phishing), 'Nigerian' scams and modem jacking are three of the most common online scams which target both small businesses and consumers.

Phishing scams have triggered a lot of media attention lately, however many consumers do not know exactly what it is. An email arrives from the bank—it claims to be updating their security information and asks you for personal information, directing you to log onto the website link attached. You log on and confirm your details. Unfortunately this a scam. The bank account is now open to fraudulent activities at your expense. You have given your password to the scammer.

Nigerian schemes were one of the earliest internet scams. You receive a genuine-looking email from an official of some distant, war-torn country. The official pleads with you to help transfer his fortune out of the country, via your bank account. You stand to make a sizeable profit from the deal, but first must pay a 'transfer fee' to help move the money. Once you send the fee, you never hear from the so-called official again.

Modem jacking is the practice of redirecting an analogue modem to a premium number, such as a 1-900 number. Sometimes email attachments, internet downloads or even websites can contain a program that copies itself onto your computer once you open the attachment. The program then uses your modem to dial a premium or overseas number, at a significant per-minute charge.

As with traditional scams, these all target the small business with its busy office, tight schedule and overworked staff. Vigilance is the best way to avoid falling victim to unscrupulous online conduct. There are also a number of preventative steps you can take to secure your computer system:

- Keep anti-virus and anti-spyware tools up to date, and scan regularly.
- Do not open email attachments unless you trust the person sending them. Be especially careful where the attachment is a program ending with .exe, .com, .bat or .scr. Most modern antivirus software will automatically scan incoming email attachments for you.
- Do not agree to website pop-ups or requests to install content on your computer unless you completely trust the source.
- Firewall software and hardware, while not generally designed to prevent viruses or spyware, can also help keep your computer safe.

There are antivirus, anti-spyware and firewall programs available freely online.

Scams and small business

Some scams specifically target businesses. Mostly, these will be online versions of the traditional directory and fake billing scams described above. However, others revolving around domain names—your website address—are also becoming more prevalent.

The National Office of the Information Economy (www.noie.gov.au) has a guide specifically dealing with this topic, titled *Staking Your Claim: a business guide to registering a web address.*

Who to contact?

Australian online scams
ACCC infocentre 1300 302 502

International online scams
www.econsumer.gov

Banking and financial scams
ASIC at www.asic.gov.au