

[The Age](#)

## [Victoria](#)

### Con artists who crash your party - or your savings

Andrew Rule & John Silvester

January 22, 2011



Who needs a gun? These days big-time thieves are more likely to come armed with electronic gadgetry. Photo: Nic Walker

GOOD thieves and con artists know that the best way to get away with the loot is to look as if you have every right to be there, doing that.

The bored gatecrasher in a dinner suit who joins the crowd of smokers outside part-way through a gala event - then produces a champagne flute, half full - has every chance of swanning inside past the gatekeepers without drawing a second glance because he's obviously been outside for a smoke. (All the better if "he" is a she in a ball gown.)

A former associate of this column, now a respectable ship's engineer, used to carry ladders and planks on his van's roof racks. With a nonchalant grunt and wave, he passed as a roadie or tradie, getting him into many a rock festival. A beanie and overalls helped mark him as bored worker, not serial scammer.

Advertisement: Story continues below

A scallywag known as "Mark of Coburg" pulled off a series of audacious stunts in the mid-1990s. No red-carpet, black-tie event was Mark-proof, from the Brownlow to Derby Day marquees. He was to gatecrashers what the young Julian Assange was to hackers, and would beat the bouncers at a given event just to win a bet.

If Mark is not in jail now, he is probably running his own conglomerate, as effrontery is a great asset in the get-rich-quick biz. The teenage Alan Bond was once sprung passing himself off as an electricity meter reader (or similar) in Perth while "casing" empty houses. This was before he graduated to spray-painting sandhills green to flog building blocks.

Then there is the delicate matter of the late father of a wealthy Melbourne businessman. The old devil was renowned in the underworld for outfoxing retail stores by ostentatiously hoisting the largest object he possibly could - once lugging a roll of carpet, legend has it - and walking out the door as if he owned it. It was the dustcoat that made him invisible, as unremarkable as a postman on his rounds. They say his light fingers, plus sly grogging and receiving stolen goods, set up the now huge family fortune.

In some settings, of course, a white lab coat would do the trick; in others, a high-visibility red or green safety vest. Such a vest is reputedly worn by a sly character seen collecting firewood in Melbourne parks, but that's another story.

These are all versions of the scam perfected by a Richmond plumbing and punting identity who considered it a matter of honour never to buy a hot water service or washing machine if he could don the magical grey dustcoat and wheel a trolley into the communal laundries of the Richmond Housing Commission flats.

Everyone assumed he was the maintenance bloke sent by head office.

But the punting plumber had his standards - he wouldn't charge age pensioners more than a cup of tea to mend a pipe or a tap. This is more than can be said of cold-hearted cyber-thieves who are getting rather good at robbing the rest of us.

According to security firms out to make small fortunes by saving corporations, banks and governments from losing large fortunes, high-tech robbery is easy if you know how. Unless, of course, soft targets are "thief-proofed" with the security firms' wonderful encryption coding gear.

Here's the scene that one security company paints. A technician of plausible demeanour - whistling as she works and wearing a hard hat and a visibility vest - puts a temporary barricade around an inspection plate in the footpath outside a building where sensitive data is received and transmitted. Treasury Place, say. Or the stock exchange or a big bank headquarters.

The "technician" lifts the plate and fiddles around in the pit, isolating an optic fibre. Then she produces a gadget the size and shape of a common paper stapler and attaches it to the fibre, then closes the pit, dismantles the barricade and saunters off. Meanwhile, the "stapler" is transmitting massive amounts of data to a laptop or smart phone left in the pit for a few hours. After that, the sky's the limit. If the "tap" hits the data mother lode, cyber crooks in a flat in eastern Europe - or East Brunswick - can download enough information - from names and addresses to bank account and credit card details - to launch a thousand scams.

One security firm touting its encryption devices - "just a box at each end of your network" - paints a scenario in which information transmitted from a corporate treasury to its bank is intercepted by what is known in the trade as a "man in the middle". He hooks into the system, changes sums transmitted by a huge amount, then drains an account before the alarm is raised - a cyber version of the old racing scam portrayed in *The Sting*.

"Add a couple of zeros to a half-million-dollar transaction and then they steal hundreds of millions of dollars in a few minutes," says Graeme Kemlo of Senetas, a security outfit that lobbies governments and corporations to buy its security hardware. "No guns, no masks, no notes - they can do it from their own bedrooms. That's what is happening in the cyber underworld: stolen money transmitted to hundreds of bank accounts they then hit with cards at ATMs to turn into cash."

The cash cards, of course, are bogus: built of fake identities from stolen passport and driver's licence and credit card details.

Apart from hacking knowhow, all a cyber bank robber needs is a "fibre tap" - the stapler-sized device described above.

"The first one we saw was made of plastic and came from Canada and cost about \$1000," Kemlo says. "It tended to break optic fibres it was attached to. But the next one was a beautifully made device from Lithuania, milled from aluminium and only half the price."

This means the cyber bank robber's "gun" costs about 500 bucks - much less than a black-market handgun in this country. And perfectly legal: you don't have to be an authorised security company to buy one. By mail order on the net, naturally.

When Senetas imported the Lithuanian fibre tap, it sent technicians to Canberra to demonstrate it to federal ministers. In a few minutes, Kemlo says, they showed that the government's ICON intra-government communications network is insecure. Which means most of us will be, too.

Somewhere out there, a cyber gang with a laptop and a fibre tap is on the prowl. You can only hope they pick on Bondy or the other dodgy billionaire whose father thieved a fortune.

Poetic justice.