



COMPUSAFE

electronic asset security

COMPUSAFE
P.O.Box 2112,Hillcrest,3650,Kzn
Reg.no 2002/071148/23
Vat no: 4710203334
Office: +2731 765 3153
Fax: 0866403151
Email: info@compusafe.co.za
Web: www.compusafe.co.za
Ian Colls – 082 4519338
Jeremy King – 071 561 3093
CIC- 0861-623-646
SAPS - 10111

Get proactive, not reactive!



Date:	13 August 2008
Author:	Cheryl Goodenough
Headline:	Identity theft and your computer
<p>REPORTS are received on a regular basis of houses or businesses being broken into and laptop and desktop computers stolen.</p> <p>Business Against Crime's manager for KwaZulu-Natal, Jody Nair, said the item of choice during break-ins at businesses was computer equipment. In addition, laptops were targets of smash-and- grabs, as well as thefts when the owners were carrying them in any busy areas, including airports and streets.</p> <p>"Laptops, in particular, are easy items to get rid of as they are very fast moving. You can sell them anywhere and they are easy to get away with as in many cases it appears as if the criminal is simply walking along with a bag," said Nair.</p> <p>A Durban company that specialises in computer anti-theft security devices, Compusafe, stated on its website that the theft of computers from businesses was especially prevalent in the manufacturing and distribution sectors.</p> <p>"It is almost a given that, at some time, a 'hit' will be made on any manufacturing operation that has vital intellectual property on a computer. The potential for disaster is much greater when there are lots of computers."</p> <p>According to Compusafe, premises in industrial areas are hardest hit, even where they have alarm systems and armed response. The biggest risk that organisations and individuals face when a laptop or desktop computer is stolen is identity theft, according to computer forensic expert and Exactech managing director Antonio Poee.</p> <p>Identity theft occurs when someone uses another person's personal information without his or her consent to commit a crime, such as fraud or theft.</p> <p>Poee warned that it was not only computers that were at risk. Speaking at a meeting of the Association of Certified Fraud Examiners in Durban recently, he said modern cellular phones and other mobile devices were sufficiently technically advanced to have the same risk.</p> <p>Devices such as iPods could be used as calendars and information could be saved on memory cards from devices such as digital cameras. As a result these devices could be targeted for the information they contained.</p> <p>A criminal might use important personal information that could be found in e-mails, calendars and office documents to impersonate a victim in order to commit the crime.</p> <p>"This impersonation can also extend to banking information since some people store credit card and Internet banking information on their computers," Poee said.</p> <p>Compusafe warned that a stolen computer might be sold for only a few hundred rands, but the information it contained might enable syndicates to plan other crimes such as armed robberies, hijackings, housebreaking, internet fraud and industrial espionage.</p> <p>The website warned that information that might be used by the theft syndicates included:</p> <ul style="list-style-type: none"> • A list of suppliers with address details and amount spent; 	

- A list of clients with address details and turnover received;
- Staff information - names, salaries or wages, addresses, telephone numbers, family members, schools, banking details;
- Accounts data - turnover, cash flow, bank reconciliation, credit card details;
- Payment methods - cash, cheque, internet, credit card;
- Classified information - designs, tenders, mergers, investments, shares;
- Stock valuations on and off site;
- Distribution and delivery network systems and patterns;
- Fleet and personal vehicles;

and

- Lists of passwords that were often left on hard drives.

So what can happen if your computer or another mobile device has been stolen? Poee said there were a number of ways that you might find out that you had been impersonated by an identity thief.

These included calls informing you that your application for credit had been approved or rejected when you had not applied for credit; getting calls from creditors following up on payment when you did not have an account with that organisation; and the presence of unknown withdrawals and transfers in your bank statements.

Industrial espionage was a serious risk for businesses.

"This occurs when data recovered from stolen **computers** is sold to competitors or used against the company to which the data belongs," said Poee.

He warned that data could also be stolen over the wire or wireless networks, making it imperative for businesses to regularly perform self-check audits and study available logs for unusual user behaviour.

Tips for organisations

- Implement a strong password policy.
- Consider using full disk or file-level encryption.
- When upgrading, donating or otherwise discarding old **computers**, make sure the data is professionally deleted.
- Perform regular security audits, including penetration tests.
- Review computer logs.
- Conduct information security training and awareness with staff who use **computers**. - Antonio Poee

Tips for home users

- Set a BIOS and operating system password.
- Make use of strong passwords to protect confidential documents, including access to your e-mail application (such as Microsoft Outlook or Lotus Notes).
- If you are going to sell or discard your computer, make sure that the data is deleted using an overwrite facility (data deleted by pressing a "delete button" can be recovered).
- Never keep a "password file" containing all your hard-to-remember passwords on your computer.

Successes

Members of the police dog unit in KwaZulu-Natal arrested 171 suspects during stop-and-search, roadblocks and cordon-and-search operations held recently. The suspects were arrested for cases including murder, armed robbery, robbery, housebreaking, theft of motor vehicle, theft out of motor vehicle, theft, rape, possession of suspected stolen property, malicious damage to property, assault,

possession of unlicensed firearm, possession of drugs and petty offences. Six unlicensed firearms, 14 stolen vehicles, four pieces of crack cocaine, two grams of cocaine and 441.93g of dagga were recovered.

Events

Drug education and awareness will be the subject of a presentation at the Westville community police forum meeting at 6pm on August 19. Guest speaker Allan Wohrnitz is the KZN representative and regional co-ordinator of Leadership Training and Drug Education to the Youth. Parents are invited to bring their children to the meeting, which will be held at the Westville Civic Centre.

Telkom scam

Another warning about the Telkom scam, and this one has been handled by Telkom's fraud department: A KwaZulu-Natal organisation received a telephone call from a person purporting to be a Telkom accounts department staff member, asking for the organisation's bank details so they could refund an incorrect debit of a couple of hundred rands. After giving the bank details, a large amount was deposited by cheque, followed by a telephone call explaining the "mistake" and asking the organisation to refund the money, less the couple of hundred rands supposedly owed. Bank account details and a fax number of proof of payment were provided over the telephone, but the organisation realised that it was a scam. The organisation is about R200 poorer as a result of the bank charges on the unpaid cheque, but Telkom is following up the report.

Telkom's fraud department can be telephoned at 086 012 4000.

Warning

Reports of games involving "beat me" and "rape me" scenarios have been received by Life Talk Forum. A recent newsletter by the forum stated that e-mails had been received regarding the growing popularity of these games.

"A sad reflection of the current times, it appears that pre-teen children (and some teens too) are role-playing some of the more drastic events that take place in our society," the newsletter stated.

"Whereas the violent and 'drastic' elements seem to vary in the different games, some counsellors express great concern about the effects that these games may have on children's behaviour patterns."

The forum requested feedback or information of personal experiences of such role-playing be sent to it at forum@lifetalk.co.za.

Tip

Fit "spacers", locks or bolts to sliding doors to prevent them from being lifted off their tracks (the most common method used by burglars on sliding doors and windows). Ensure all windows are fitted with adequate locks or burglar bars that cover all glass. - ADT Security