



Organised crime... global problem...

Think phone fraud, phreaking, toll fraud, long distance hacking, telecom fraud, PBX fraud isn't a problem?

Think again.

Large company, small company; to these criminals it doesn't matter.

This could easily happen to your business, or your customers.

The following phone fraud evidence is compiled in chronological order.

Phone Hackers Target New Zealand Firms 6 April 2010

Boehringer Ingelheim (pharmaceuticals) and about 40 other affected customers of Telecom, as well as more customers from TelstraClear, were hacked. TelstraClear sees at least two cases a week in New Zealand. Both telcos recommend password protection, but passwords can be cracked in milliseconds by hacking software – telco providers do not have a solution, and do “not have a blanket policy of waiving the charges of scam victims”.

UK among global leaders for telecoms fraud, which runs at \$80 billion worldwide 11 Mar 2010

Distributors of Control Phreak (by The Callista Group), Nimans and Rocom, are now at the forefront of attempts to contain telephone hacking in the UK. Phreaking/phone hacking/PBX fraud is even linked to terrorist groups, who use telecoms fraud to raise illegal funds. Control Phreak now comes with an integrated Proxy Server that only allows authorised access to PBX programming, and provides total 24/7 protection, automatically detecting and killing illegal activity

UK in top 5 for global communications fraud, says CFCA 11 Mar 2010

The UK has joined Cuba, the Philippines, Lichtenstein and India where the biggest telecom fraud problems occur says Communication Fraud Control Association (www.cfca.org). However, Nimans and Rocom are distributing Control Phreak (by The Callista Group), a fully automatic PBX firewall – and the only software based program of this type on the market – that stops telephone hackers from making expensive international calls, which land unsuspecting companies with huge bills.

[Adelaide Business Defrauded of Up To AU\\$100,000](#) 23 Feb 2010

Adelaide business scammed of AU\$100,000 through their breached PBX. Security expert recommends changing default passwords, but this will not protect against phreaking.

[PBX Fraud Strikes Toronto](#) 1 Dec 2009

A Toronto marketing firm was phreaked for over CA\$70,000 and their telco provider, TELUS, failed to block outgoing toll calls after the firm contacted them to help stop it. TELUS says that because they have to pay, the phreaked businesses have to pay too. Article suggests password protection, but this can be broken with modern code cracking software very easily (as proved by other articles).

[Internet Phone Systems Become the Fraudster's Tool](#) 27 Oct 2009

The hacked telephone systems of small to medium-sized businesses were used to gain access to bank customers and trick people into divulging banking information. Banks such as Liberty Bank and Union State Bank.

[Toll Free PBX Hack Highlights Need for Code Auditing](#) 2 Sept 2009

A North Carolina, USA, business left with a US\$2,500 phreaking bill. This article talks of code auditing to help secure systems, but passwords and code security can now easily be cracked by new hacking software tools that are freely available online.

[Australian Channel Nine News Video on Phone Hacking](#)

A news segment on phreaking, featuring an interview with a hacker about how easy it is to run up AU\$20,000 in just one night. It takes about 5 minutes to hack into someone else's line, and would-be criminals can download the necessary software off the internet for free, easily. (This is direct line phreaking, a type of phone hacking.) This hacking helps to fund Australian organized crime and is estimated at costing Australian companies up to AU\$78,000 a day. Telstra says they refer cases to the police, but customers are responsible for their own security and bills.

[Gamma Telecom Aids PBX Resellers' Fight Against Telephony Fraud](#) 24 Aug 2009

The telco company Gamma Telecom proposes alerts when customers' calls exceed pre-set limits, but this will still allow fraudulent charges up to this limit, and customers will still have to pay for these fraudulent charges.

[PBX Security: Understanding the Real Threats to Your PBX](#)

Proctor and Gamble phreaked for US\$300,000. Sumitomo Bank for US\$97,000. New York City Human Resources for \$704,000. Tennessee Valley Authority for \$65,000.

[Notorious Phreaker Gets Sentenced to Eleven Years in Prison](#) 30 June 2009

19 year old phreaker from US sentenced to 11 years in jail for phreaking, listening in on phone calls, fake 911 calls, harassment, and attempted blackmail. Another co-phreaker sentenced to 18 months. Responsible for many incidences of "swatting", sending SWAT teams out to locations unnecessarily due to faked 911 calls. Committed phone fraud against Verizon and AT&T to avoid paying his own large phone bills.

[Alleged Hacking-Terror Effort Thwarted](#) 13 June 2009

Wall Street Journal article about a cracked US\$55 million phreaking ring. This article contains Grand Jury indictment PDF and info about the al Qaeda terrorist links. Linked to the same group that financed the communications behind the Mumbai terrorist attack in which 170 people were killed. They conspired to break into the phone systems at 2,500 entities in the U.S., Canada, Australia and Europe.

[International Phone Fraud Ring Busted](#) 15 June 2009

Article about the same US\$55 million phreaking ring. Italian call center operators were paying the hackers around \$100 for each hacked PBX. The operation lasted from October 2005 to December 2008. Access was also sold to illegal operators in Spain and other countries. The hacked calls totaled over 12 million minutes.

[PBX Hacking Moves into the Professional Domain as Arrests Stack Up](#) 15 June 2009

As above. Hacking ring cracked, international arrest warrants issued from Italy. Companies in USA, Australia and Europe hacked. AT&T (hit for US\$56 million) talks about their customers being phreaked by hackers using sophisticated code breaking software. PBX access codes were being sold for US\$100 a piece and funds went to extremist groups.

[Bell Canada Customer Billed \\$207,000 after Hacker Breach](#) 27 Jan 2009

Toronto businesses angry that they've experienced toll fraud to the tune of over CA\$200,000 and Bell Canada expects them to pay the bills. Bell Canada claims the problem is rare (it isn't) and says that passwords will offer adequate protection (they don't, as the phreaked businesses point out in the article).

Bell Canada admits it's an international problem, but says it's their customers' responsibility, not theirs (a stance taken by telco providers generally).

[Has associated CBC News video.](#)

[Phreakers Hit Australian Companies](#) 22 Jan 2009

A Western Australian company was phreaked for over AU\$120,000 when 11,000 hacked international phone calls were made in only 46 hours. The company's normal phone bill was only around AU\$500 per month. Hacking ring likely, rather than an individual. Information about hacked PBX systems is often sold to other hackers, so the phreaking cycle continues.

[Firms Face Rise in Phone Fraud](#) 01 Jan 2009

Irish business have increasing, expensive, trouble with phreaking / PBX hacking. (Sometimes the article can be viewed without subscription, sometimes not).

[TelstraClear Fraud Department Warning](#)

You are responsible for your PBX security, and any illegal charges if you are phreaked, says TelstraClear, telco provider. Says phreakers are highly skilled sophisticated criminals, who are conducting a growing worldwide business selling illegal phone access. Phreakers hack big and small businesses, and losses average from NZ\$10,000 to NZ\$100,000 plus per incident. Reiterates that your security is your own problem.

[Voicemail Hack Costs Business Owner \\$43,000](#) 22 Dec 2008

Canadian company received a CA\$43,000 phreaked phone bill after hackers made hundreds of calls to Bulgaria. The business owner was upset that the telco provider assumes no responsibility and did not alert him to extremely unusually high phone bill. The business owner compared it to credit card fraud, where a credit card company would automatically alert a customer to such unusual charges and said that telco providers lack adequate consumer protection. The business owner may have had to fire an employee in order to be able to afford to pay off the bill.

[Suing for Poor Performance](#) 12 Dec 2008

A small business was the victim of dial-through fraud for £22,000 and owner wanted to sue his telco provider for poor or non-performance of service contract, because of an unprotected remote switch and no mention of the vulnerabilities of this in the training or user guide.

[Telecom Frauds Not Taken Seriously by Companies](#) 29 July 2008

Survey of 250 organisations found 40% had experienced telecoms fraud. Yet companies still dangerously believe this will not affect them.

[Nortel PABX Hacked Again](#) 19 April 2007

Legrand Software, a Sydney company, was phreaked for AU\$1,800 of illegal calls to Algeria in one night. Their PBX provider never made them aware that this sort of hacking was a possibility. They said that their telco providers Optus and Telstra were very unhelpful and unable to stop the calls once they were discovered. Said these telco providers put the problem into the “too hard basket”.

[Telephone Hack Costs NSW Firm AU\\$9,000](#) 17 Oct 2006

A small Sydney business was phreaked for AU\$9,000 – eight times more than their usual phone bill, very damaging to a small business. Illegal calls were made to the Arab Emirates, Somalia and other countries in Africa and South America. Article admits phreaking is a common problem, but companies don't want to admit to being phreaked out of embarrassment over security.

[Feds Arrest VoIP Exec for Wire Fraud, Computer Hacking](#) 8 June 2006

The executive of two Florida VoIP companies who made a business of hacking into other providers' networks and routing his customers' calls onto those platforms, arrested for fraud. Over US\$1 million in illegal profit. Some companies billed for over 500,000 illegal calls that he then sold on. This is business to business fraud, but it shows extent of telco fraud in all sectors. He could face max 20 years in prison for wire fraud, or five years in prison for computer hacking, plus fines.

[Phreakin' Hell: Phone Hacking Costing Australia Millions](#) 23 Nov 2005

Phreaking costs some companies up to AU\$1 million in single attacks. Companies don't want to report this fraud out of embarrassment over security. Perpetual Trustees was phreaked for AU\$600,000 (including AU\$80,000 in one day) due to 5,000 illegal calls. A Canberra private hospital was phreaked for \$4-5,000 in 24 hours. An organised phreaking ring likely, rather than an individual. Plastic Plumbing Supplies was phreaked for over AU\$50,000 and had to pay it all as their telco provider threatened legal action. Telstra admitted to 20 hacks a month against its customers in 2005, and this will have more than doubled as other companies will no longer be with the now privatized national carrier. Phreakers don't discriminate between small and large business, and illegal charges can be enough to bankrupt.

[Siemens Press Release on Rising Telephony Fraud](#) 9 Nov 2004

Siemens admits PBX fraud a huge problem exceeding £40 billion worldwide annually. One of the few PBX providers to admit to this worldwide problem, but does not give airtight solution.

[Filipino Phone Phreakers Foiled](#) 20 July 2004

A gang of phone phreakers from Manila had been hacking the Philippines' main telco provider (Philippine Long Distant Telephone) and its customers for millions of dollars over 6 years. Philippines' military said these telephony criminals had defrauded the government out of over \$20 million pesos in expected revenue, and that the level of this crime was tantamount to economic sabotage for the country.

[McAfee informative PDF on VoIP fraud.](#)

Other evidence from Callista's [Control Phreak presentation](#):

Telecom Fraud in the **UK alone costs £1.3 billion yearly** (Comms Dealer (UK), January 2009 / BT / TUFF) and **40% of UK companies** have experienced it (Network World / Davomo UK / Redshift Research, July 2008).

Telecom Fraud is estimated at **US\$52-60 billion per year globally** and is still **growing, at 15% per annum** ([Communication Fraud Control Association](#). Peter Hoath, BT, Seminar on Costs and Tariffs, January 2008. [APACS Press Release](#) 19 March 2009. Also ComReg Ireland press release, 12 May 2009).

Irish Department of Social Affairs was **phreaked for €300,000**. MinuteBuyer (Ireland) client **defrauded of €40,000**. World Trade Group (London) **phreaked for £27,000 over one weekend** (Silicon Republic / Auditor General, Ireland; Enterprise Ireland, eBusiness Live, March 2009).

The Callista Group Limited | Global Development and Support Centre
PO Box 34480 | Auckland 0746 | New Zealand
Tel +64(0)9 4810377 | Fax +64(0)9 4805775 | support@callista.net | www.callista.net

The Callista Group Limited | UK and Europe Sales and Support Centre
Westcott Barton | Oxon | United Kingdom
Tel +44(0)1869 340 252 | support.uk@callista.net | www.callista.net

Callista, Calyx, Calcue and Control Phreak are registered trademarks of The Callista Group Limited.
Copyright © 2010 The Callista Group Limited



UNITED KINGDOM & EUROPE

Nimans Ltd | www.nimans.net | Tel: +44 (0)844 848 0900
Agecroft Road | Pendlebury | Manchester | M27 8SB

