

Control Phreak

A C T I V E • V O I C E • S E C U R I T Y

A Compilation of Phreaking Evidence

January 2012

Callista and Control Phreak are registered trademarks of the Callista Group Limited.
Copyright © 2012 The Callista Group Limited

The following phone fraud evidence is compiled in chronological order, with links provided.

12 Jan 2012

Hacked Asterisk PBX

Tom Keating has experienced hacking on his PBX and found a company with something “mighty fishy” going on. He thinks that “Perhaps their business model is to crack Asterisk boxes and resell the minutes”.

9 Jan 2012

Warning! Phreaking!

A long-time member of the forum EduGeek.net writes:

“Seems to be PBX hacking is on the increase & has spiked over the last 3 - 6 months. 2 forms that are linked, either the PBX gets rooted to be a step in a chain and forwards calls to a local number, increasing your bill slightly but maybe not so much as you'd noticed, or you end up being the final step in the chain, a number is routed to some far flung corner of the globe and you get whacked with anything from £1000 upwards, with costs of £10k or £30k. Seems to be a lot of uncertainty on how it happens but has happened to non-IP connected devices so it is not just a computer network issue. We have been advised that basically PBX's cannot be trusted to be secure so anything implemented on them (forwarding blocks, locks, passwords) can be bypassed & anything else is reactive so you still get the costs racked up.

The only solution given to us is an external service (installed on our server) that monitors the PBX actions and follows rules on whether it allows it or not. Anti Virus for phone systems!! Be careful out there!”

6 Jan 2012

Hambleton Businesses Wary of Expensive Hacking

Police in Hambleton, UK, have warned business owners about the risks of toll fraud following a local company being hacked for £20,000.

Says Ross Knapman of Deep Blue Telecom, “Once access has been gained to a company’s network, this can be used to illegally route calls, either to make international calls or even to generate revenue from premium rate numbers, all at the expense of the hacked company. It is the latter that has recently been done to some companies in the Harrogate area... The average call charges faced by a company hit by this type of hacking is £10,000, but one company that was hit over the New Year weekend had £25,000 of call charges generated.”

2 Jan 2012

South African VoIP Services at Serious Risk

VoIP is just at risk of hacking as are bank accounts or the internet, companies are discovering. When companies are hacked, they are liable for the illegal charges. Even network operators that are aware of the problem can at best promise that they have a service that “limits the risk somewhat”.

A member of the related **forum** says that they were hacked for \$33,000 in 2011.

15 Dec 2011

ComReg Warns of Rocketing Phreaking Rates

PBX hacking – estimated by the Forum of International Irregular Network Access (FIINA) to be growing worldwide at 15% per annum – is on the rise, warns telecoms watchdog ComReg.

“Typically, fraudsters target firms during out-of-business hours and break into the PBX and generate calls via any one of the company's lines. IDC estimates there are more than 200 different types of PBX fraud in existence.”

9 Dec 2011

Politically Motivated Phone Hacking in Wake of Russian Election Outrage

In what is being called the most “interesting” of the many forms of hacking taking place during protests over the Russian elections, the Guardian reports that “the liberal Yabloko party and newspaper Novaya Gazeta said their telephone lines had been paralysed by endless calls featuring a recorded female voice: ‘Putin is very good. Putin loves you. Putin makes your life happy. Love Putin and your life will fill with meaning. Putin does everything for you. Remember, Putin does everything just for you. Putin is life. Putin is light. Without Putin, life has no meaning. Putin is your protector. Putin is your saviour.’ Over and over again.”

8 Dec 2011

Fed up with Constant PBX Attacks

A member of an IT security forum relates his frustration that his company is “under a constant attack on my local [number]. If I leave my phone line plugged in to my VoIP router after 3:30, I will have upwards of 1000 voice mail messages in the morning by 7am. It basically continues to try and bounce its calls through our system until the voice mail box is full. I tried working with the tech company managing the system, and they basically came to the conclusion that we need to change our number or unplug the line every night. The phone company also doesn't seem to know what to do either, I worked with a senior-level tech for a few hours, and he said the return field was being randomly generated/spoofed for each call that came through, so there was really no way for them to block them either.”

The company's phone system is “all outsourced to a third party, which stopped responding to my pleas for help a month or so ago.”

28 Nov 2011

Philippines Police and FBI Bust Terrorist Hacking Gang (also [here](#))

In a joint bust the Philippines Police and the US FBI have arrested four PBX hackers in Manila who were targeting the customers of US telco provider AT&T, among others, with the money raised being diverted to bank accounts of a Saudi terrorist organisation. The Philippines' Criminal Investigation and Detection Group (CIDG) and FBI say that the four hackers were paid by the same terrorist group who funded the November 2008 Mumbai terror attacks which killed 164 and wounded at least 308.

The loss to AT&T as a result of this hacking was nearly US\$2 million.

Chief of the FBI's Anti-Transnational and Cyber Crime Division (ATCCD), Police Senior Superintendent Gilbert Sosa, said that this bankrolling terrorist group was originally run by Muhammad Zamir – a known member of Jemaah Islamiah, a Southeast Asian militant network with links to al Qaeda. Jemaah Islamiah are thought to be behind the Bali nightclub bombings in October 2002 which killed 202 people, most of them Western tourists.

“The hackers broke into the phone systems of some AT&T customers and made calls to international premium-rate services whose payments would be diverted. Such scams are relatively common, often involving bogus premium-service phone lines set up across Eastern Europe, Africa and Asia.”

FBI officials say that the arrests are part of an ongoing investigation.

23 Nov 2011

Sky-High Cost to UK Businesses

PBX hacking is estimated to be costing UK businesses over £1b per year with the UK now in the top five "phreaking hotspots" in the world. According to the latest research from The Communication Fraud Control Association the UK has joined Cuba, the Philippines, Lichtenstein and India as one of the world's worst PBX hacking areas - with problems continuing to escalate. Its small to medium sized business that are targeted the most as they are most vulnerable. Roger Ansin, MD of Callista, interviewed by the BBC, says "Companies have to start to secure their phone systems from this; otherwise they could get hit with very large bills. The issue for them is that they are obliged to pay it, because to the carrier the calls came from their phone system. Therefore they are responsible for that bill"

The average cost to a victim of a UK phreaking attack is currently estimated at £10,000. Once the hackers have gained access to a system it becomes open to abuse time after time until the fraud is detected, by which time the damage has been done and the victims have no option other than to pay for the stolen calling hours to premium rate numbers.

Most businesses spend significant resources protecting and securing their networks and PCs from external virus, hacker and spy attacks but leave their PABX network completely unsecured and defenceless.

7 Nov 2011

Calgary Businesses Warned of Phreaking Attacks

A Calgary, Canada law firm was hacked for CA\$4,000 in long distance calls. Security officials say this happens all the time. Another Calgary company, the business advisors Stawowski McGill, were targeted in September, receiving a giant phone bill that included calls to Africa. They learned hackers had accessed the company's voicemail system in order to steal and resell phone time.

According to Bell Canada, "Canada alone accounts for about \$30 million of that [global telecommunications fraud] loss. About one in four international companies has been or will be the victim of some type of toll fraud."

7 Nov 2011

CCTS Tells Canada: Toll Fraud is on the Rise

"Canada's Commissioner for Complaints for Telecommunications Services (CCTS) yesterday urged small and medium sized businesses to monitor their PBXs for suspicious activities following a resurgence of complaints about long distance toll fraud.

The CCTS, an organization funded by the telecom industry to resolve complaints against companies in the sector, also reported that complaints about wireless and home phone services more than doubled in 2010-11 compared to what the commission received in 2009-10.

According to the CCTS's Annual Report – Restoring Connections, Canadians filled 8,007 complaints for the period between August 2010 and July 31, 2011. That was a 114 per cent increase from the previous year's 3,747 complaints, said Howard Maker, commissioner of the CCTS."

Says Maker of long distance toll fraud in Canada, "we are seeing a resurgence of these complaints in 2010-11. The bills sometimes amount to five or six figures".

26 Oct 2011

AstriCon Audience Member Experiences US\$400,000 Toll Fraud ([YouTube video here](#))

"During an AstriCon session on VoIP security the speaker discussed how easy it was to hack voicemail PINs... to initiate "call backs" using spoofed CallerIDs. Essentially, this leverages the "call back" feature that many voicemail systems have to call back the person that left the message. He then asked the audience for any real world examples of how they were hacked. Several volunteered their stories. [One] was hacked - due to their parent company locking them out of the server and not updating /patching the server. This resulted in the hackers racking up toll fraud (Korean calls) of \$400,000!"

18 Oct 2011

Fortune 500 Financial Firm Hacked by Testers

"A long-forgotten PBX field-manager user account at a well-fortified Fortune 500 financial services firm was all it took for penetration testers to set up shop and await their moment to gain access into the otherwise well-secured network."

29 Sept 2011

828 Suspects Arrested in Transnational Phone Hacking Bust

Police from the Chinese mainland, Taiwan and eight countries of the Association of Southeast Asian Nations (ASEAN) shut down two large transnational telecom fraud groups. According to China's Ministry of Public Security (MPC), the first group of 45 suspects involved in the crimes was repatriated to China from Indonesia by a police escort. A total of 828 suspects were arrested, including 532 mainlanders, 284 residents of Taiwan, and 12 others from ASEAN countries, including Indonesia, Cambodia, the Philippines, Vietnam, Thailand, Laos, Malaysia and Singapore.

PBX hacking is becoming more prevalent in China's west and northeast regions after being mostly concentrated in the country's southeastern coastal cities in recent years, the ministry said. Earlier this year, a group of Taiwan natives were found to have organized a telecom-based swindling group and set up a telecommunications fraud network throughout the Chinese mainland, Taiwan, the Philippines, Thailand, Indonesia and Vietnam. In April, another group of Taiwan natives were found conducting similar activities in Jinhua, a city in eastern China's Zhejiang Province.

The networks primarily targeted mainlanders and Taiwan residents, with a total of 220 million yuan (US\$34.41 million) involved in the two cases.

16 Sept 2011

Member of an Avaya Users' Forum Tells of PBX Hacking

A Canadian member of International Avaya Users Group posts asking for information related to the PBX hacking they're experiencing on their 100 Norstar systems. They say, "We are being attacked by toll fraudsters who are using the through dialing to access 10-10 type services which are then billing us large amounts of money. Because our systems are over a large area with no remote access it's taking time to get to them all to fix the problem. Is this happening to anyone else? What's particularly curious is that they are able to make a large volume of calls on systems with only a few trunks on them which is baffling."

13 Sept 2011

New Zealand Businesses Warned of Increased Hacking Risk During Rugby World Cup

According to the Telecommunication Carriers Forum (TCF) PABX fraud quadrupled in 2010, with 30 to companies in New Zealand being hacked by phreakers every month – to the tune of hundreds of thousands of dollars. There is a danger that PABX fraud will increase during the Rugby World Cup. David Stone, the CEO of TCF says, "With so many tourists expected to visit New Zealand, international fraudsters may take the opportunity to target New Zealand for PABX hacking during this time," comparing leaving a PABX unsecured to leaving PIN numbers or bank account details and access codes pinned to your front door. He continues, "Security of your PABX is easily as important as the security of your PC; it's relatively easy to defraud you of thousands of dollars if you haven't made your system secure."

However, despite TCF's recommendations, evidence shows that passwords, auditing and the like are no real protection against phreaking.

15 August 2011

BBC News item on Look East: Businesses Being Hit by Phreaking (video)

This cybercrime is costing businesses across the eastern regions of the UK thousands as computer hackers re-route international calls through company switchboards. The sophisticated scam, known as dial-through fraud or phreaking, usually originates overseas.

A business in Basildon, UK, was hacked to the cost of over £1,600 in illegal calls to Papua New Guinea. The company, Connects Ltd, are themselves installers and maintainers of telephone networks – and thought that phreaking was something that happened to other people such as customers who didn't follow Connects Ltd's advice. Connects' George Georgiou says, "We'd felt our phone system was bullet-proof... it [the fraudulent phone calls] was four times our annual phone usage... it's a lump. We're never ever going to get it back... If you're a start-up business and you'd been done for £1,600 [or] £3,000 that could cripple you."

Of the £40 billion annual global cost of phreaking, £1.2 billion is from the UK.

Roger Ansin, MD of Callista, is interviewed by the BBC about PBX hacking. He says, "Companies have to start to secure their phone systems from this, otherwise they will get hit with very large bills. And the issue for them is they are obliged to pay it, because to the carrier the calls came from their phone system. Therefore they are responsible for that bill." Critics of telcos say that because the blame and bill is placed on the customer, telcos have little motivation to stop phreaking.

15 August 2011

VoIP a Handy Tool... With Risk of Fraud

David Cargill, council member for the **ITSPA** (Internet Telephony Service Providers' Association), says that while the benefits to VoIP and an IP PBX are great, so are the possibility of PBX hacking. Adequate security is a necessity.

9 August 2011

Monster PBX Fraud Nightmare Compounded by Bad Telco Treatment

Cynthia Elkins, an employment lawyer from Woodland Hills in Los Angeles, California, has found herself in the middle of a phone hacking nightmare worth over US\$20,000 – all illegal calls made to places like Israel, Egypt, Saudi Arabia and Palestine. Her carrier AT&T has dragged out the situation for nearly a year, advising her to ignore the calls and then in an about-face, demanding she pay the fraud bill and even making the glib comparison that “If your toaster blows up in your home, you don't expect the electricity company to be responsible for it, It's your toaster” (John Britton, AT&T spokesman).

Elkins says, “I'm so disgusted. They're [AT&T] just taking advantage of a small-business owner. It makes me wonder how many other people they've done this to... I spent in excess of 25 hours trying to resolve this and pulling my hair out in the process.”

Yet, an AT&T service representative admitted to Elkins that “this happens all the time”, and she says that initially “I was told that it was obvious these weren't my calls and I wouldn't be held responsible. AT&T made it clear that I didn't have to worry about it.”

Over a period of months she received similarly contradictory information from the telco – that she needed to pay up within three days or face disconnection, and then that she didn't need to worry about it. Finally AT&T told Elkins that they indeed considered the bill her responsibility.

While credit card companies do not expect defrauded customers to foot the charges, this is not the case with telcos. Verizon also expects customers to pay for PBX fraud bills. Though AT&T says they have resolved things with Elkins, she intends to inform them that she'll be switching phone companies.

3 August 2011

Ireland's COMREG Sees Huge Increase in PBX Fraud

COMREG has seen a big increase in complaints about phone hacking with 21 complaints in Ireland so far this year, which was the figure for the entirety of 2010. These figures are up from 19 in 2009. These reported attacks alone have cost Irish businesses €620,000 in the past two years. COMREG says that these criminal calls often happen after office hours.

19 July 2011

News of the World Hacking Reminds Phreaking Victims of their Experiences

New Brunswick PBX hacking victims had unpleasant memories brought back by recent events in the UK. Bob Pritchard of Saint John, New Brunswick, Canada **had his PBX hacked in March 2011**, with the criminals racking up CA\$10,000 in illegal long distance calls and his telco being actively unhelpful. Pritchard says, ““First of all, you're talking about a criminal act. Any information that your computer or your phone system is collecting, which would be all of your inbound calls, all of your outbound calls, all of your voice mails, could all be accessed by the person breaking in.”

Another phreaking victim from Saint John, Kalyn O'Neill, says, "It made me really nervous because I didn't realise how easily it was done and how fast it could happen.”

19 July 2011

Phone Hacking of All Types Getting Easier for Criminals

Experts say phone hacking is becoming easier and more lucrative for phreakers. Many suggest security measures such as auditing and changing passwords, but as ex-hacker turned security consultant and writer [Michael Calce](#) says, "This will only minimize risk, hackers are constantly writing software that phone companies don't know about."

[Unlike Control Phreak, which easily and automatically solves this PBX phreaking problem.]

18 July 2011

West Virginian Small Business Receives Shocking Phone Bill [also [here](#)]

Staff of Global Tech Communications, a division of Advanced Electric Inc. in Kanawha County, West Virginia USA, were stunned to receive a phone bill for US\$9,238 – when their usual phone bill is US\$350-400. Office manager Sherri Mace comments, "I almost passed out." Illegal long distance calls were made through the company's hacked phone system to places such as Libya, Israel, Afghanistan – and even the Vatican. This amounted to a phone bill with 12 pages of illegal calls – more than 1,500 calls in total. Mace says, "If you look at the time that they were made, it's every five or ten minutes. They just keep, non-stop, 24/7 making the calls... You don't expect to pay that much for telephone – ever. Hopefully, ever."

As the US Attorney General's office says, this is known as phreaking. Matthew Stonestreet, assistant attorney general with the Consumer Protection Division reported that "[the criminals] can spoof themselves as your account and from a phone far away. It doesn't have to be on site. It can look like these calls are coming from your businesses or from your home." He also warns, "The problem with phone lines is a lot of them aren't encrypted and they don't have firewalls up, and computers do."

Luckily for this business their telco FiberNet – who said that this had happened before – erased the illegal charges. But unfortunately for most phreaking victims, this telco attitude is a rarity.

18 July

PBX Fraud Still on the Rise

A company in South Africa is beginning to inform people of the risks of PBX fraud. "Statistics indicate that PBX fraud is on the rise and growing in volume and sophistication... Often the cost to company associated with this type of fraud directly relates back to lengthy or international calls being made on the PABX system – ones that are being charged back to the organisation and in most cases are not picked up by the business."

Resellers, carriers and the like may advertise that they monitor international calls and alert customers to unusual traffic, but as the company themselves admits, "However, ultimately it is the responsibility of the organisation to monitor such potential security flaws in their PABX."

8 July 2011

News of the World Cellphone Hacking Scandal Highlights Phreaking Problems

Recent mobile phone hacking in the UK has highlighted how encompassing the problem of phone hacking is. This includes criminal activity "such as hacking corporate PBX systems to initiate outbound calls to premium numbers". Software to allow this is freely and easily available online. According to the CFCA PBX/voicemail fraud accounts for about US\$15 billion annually.

15 June 2011

Vancouver Business Hacked for CA\$4,000

Local police are investigating a business being hacked through their PBX over a period of days from May 30. Police “found methods on how to compromise the system are available on the internet, most commonly by hacking the computer and gaining administrative access using the manufacturer’s default password.”

14 June 2011

Essex Company Loses £3000 to PBX Hacking [video interview [update](#)]

Jenny Boreham, owner of Fastsigns in Chelmsford, Essex, had her business line hijacked to make illegal international calls between 1 January and 30 April. She only discovered this phreaking after receiving a huge telephone bill. Boreham says, “I find it incredible this is happening on a worldwide basis and it can cost people an absolute fortune. I have been told... passwords do not protect you. At this time people cannot afford for this to happen to them.” Additionally, PBX system providers do not feel that they are responsible for this sort of security breach – customers are by themselves.

She remains unimpressed with poor security information, saying in a TV interview, “I was also informed that actually my bill was at the lower end of what happened, and that actually I was quite lucky.”

13 June 2011

Growing Threat against Unified Communications Systems

According to recent reports attacks against unified communications are increasing. For example:

- “... 50% increase in attacks from 2009 to 2010 from hackers targeting enterprise UC servers (source: VIPER Lab honeypots).
- Now up to 25% of all hacking attacks in the wild (open Internet) are against the voice and UC vector, up from single digits in previous years (rest of attacks are classic database and network layer attacks).
- An attack against VoIP takes place every 2.5 minutes during peak periods (source: VIPER Lab).
- More than 20,000 exploits and threats against VoIP and UC are now identified.
- More than 2,200 enterprises in US compromised by a single team of hackers in voice toll fraud attacks that stole \$55 million (source: US Federal Bureau of Investigation).
- Romanian hacking ring hit businesses with VoIP attacks **stealing 11 million Euros** (source: European Law Enforcement authorities).
- Thousands of examples of enterprises compromised because inadequate SIP trunk, VoIP server protection (sources: multiple, including Network World magazine, Unified Communications magazine, Comms BusinessMagazine, FierceVoIP, others).
- ‘Call walking’ reconnaissance attacks, scanning attacks make up majority of VoIP attacks against enterprises, precursor to toll fraud ...”

26 May 2011

Telecoms Fraud Suspects Returned to Taiwan

“Returning the suspects is based on a cross-Strait agreement on the joint combat against crimes and judicial assistance. Police forces from the Chinese mainland and the Philippines cracked a major transnational telecommunications fraud ring late last year. On 2 February 2011 the mainland police escorted 24 suspects in connection with the fraud back from the Philippines, including the 14 Taiwan residents.”

14 May 2011

Phone Line Hijacking Costs Small Business Nearly CA\$17,000

15 person small business Prototier, an automotive prototyping company in Alliston, Ontario, Canada has been hit with a CA\$16,918.57 bill for 1,195 illegal long distance calls to Tunisia over a three day period in late March when the company office was closed for a trade show. Their usual monthly phone bill is usually only CA\$100. Tina Rousseau, Prototier project co-ordinator says, "We're going to fight the bill. We don't want to pay it. We don't even want the insurance company to pay it." Rousseau also says that Bell Canada should be responsible for the bill as they own the phone lines, and that telephone companies should be better informing their customers about PBX fraud. However, Ontario Provincial Police Constable Peter Leon said it's unlikely that Prototier's service provider will have to foot the bill. Rousseau says she had never heard about this type of fraud cases until it happened to her, and doing her own research after the fact she discovered it is more prevalent than she ever imagined.

7 May 2011

Phreaked Businessman Wants More Done Against Toll Fraud

Martin Aitken, owner of Aitkens Pewter, is angry at authorities after he was hit with a bill for CA\$1,563.24 in calls to Zimbabwe that he didn't make.

Aitken says, "Today, there is a lack of interest in addressing this particular problem. The phone companies are just sort of saying, 'Yes, yes, you've been hacked, you've been robbed.' The guys who install the phone systems say, 'Yes, it happens all the time.' And the police say, 'Yes, there is nothing we can do about it'. He would like to see toll fraud charges reversed and taken seriously in the same way credit card fraud charges are.

However the Public Affairs manager for telco Bell Aliant says that "the owner is still responsible for charges made on their line" and they will determine if the customer will be responsible for the whole charged amount or a portion. Either way, the phreaking victim will be footing some of the cost of the illegal calls.

2 May 2011

Man Tells of His PBX Being Hacked

A member of the dsreports.com forum tells other members that his PBX was hacked. He started getting automated low account balance reports from voip.ms about his SIP account and was surprised to discover that the problem was phreakers. Voip.ms informed him that because the hackers were flooding his account, it wouldn't be able to be automatically cut off once his account balance reached zero, as it was supposed to. The hackers called multiple overseas numbers, testing the system, before installing an automatic message that would hold the line open for as long as they liked. This happened despite the forum member's password being extremely complicated.

He says, "Moral of my story... Never think it can't happen to you. Just when you think you've crossed all the Ts and dotted the Is. Also as a quick thing, be careful with your SIP provider. Even if they are pre-paid and cut you off on zero balance, doesn't mean it can't happen the way it did to me."

Other members respond that this hacking has also happened to them multiple times.

29 April 2011

Another Canadian Business Phreaked for Big Bucks

A business in St. Clair Township, Canada was stung with a shocking CA\$130,000 phone bill after illegal calls were made to Tunisia through their phone system over three days in March.

30 April 2011

Famous Former Hacker Hired as Security Chief [Italian publication]

Jeff Moss, known online as 'Dark Tangent' was hired by multiple security organisations, including ICANN and Secure Computing Corporation, and is the founder of 'Black Hat', an annual conference on information security in the USA. Having been a phreaker in the past, he is now in demand by companies who understand how much of a threat PBX hacking poses.

21 April 2011

International Hackers Target Australians

The Bleeding Edge group in Sydney was targeted by phone hackers, who gained access to their system and made calls to Latvia, Romania, London, and the Solomon Islands among other locations. They say, "We should have picked that up earlier but we'd been lulled into a false sense of security. In December, the tech-support people at Australian Technology Partnerships advised us to improve the security on our Asterisk open-source phone systems, which uses the VoIP lines, because they'd heard some unpleasant stories about local businesses being charged many thousands of dollars for fraudulent calls that had been placed through their PBX systems." They made recommended changes to secure their system – such as altering passwords – after learning of a case where a Perth business had been hacked for AU\$120,000 (see the example in this document, Phreakers Hit Australian Companies, 22 Jan 2009).

However, they were hacked again, and then a third time. They have had to bar international calls on their VoIP lines, not an ideal solution for ongoing business.

21 April 2011

The Need for Adequate Voice Network Security an Increasing Concern

"A major U.S. based Service Provider went through a two-day, SIP-based, Telephony Denial of Service (TDoS) cyber-attack... With the advent of Voice over IP technology, enterprises are increasingly exposed to voice-based IP attacks such as... toll fraud... Today's companies face increasing costs as they struggle to handle the enormous volume of fraudulent calls. Adding resources (people, systems, space) and upgrading equipment can only go so far. At the same time, customer satisfaction drops when response time slows – and the company's brand takes a hit."

Companies need to stay ahead of hackers if they want their systems to be protected.

19 April 2011

Calgary Family Business Phreaked (also [here](#))

A couple from Calgary who run a small accounting business were hacked over less than 12 hours for CA\$1100, with illegal calls being made to Tunisia. The phreakers gained access by dialing the remote voicemail access number on the couple's system and hacking their password. Their telco, Telus, held the couple liable and they had to pay the illegal bill because Telus considered the problem a weakness in the couple's equipment. However, the criminals dialed out to Tunisia using a feature the couple didn't even know they had. This is typical of phreaking incidents: customers are not adequately informed of the security risks, are given poor advice (such as using passwords, which can easily be hacked even if they are over ten digits long), and then are held liable by Telcos for the bill. The couple was also told by their system provider that several other Calgary businesses were phreaked over the same period.

19 April 2011

VoIP Security Risks Demonstrated at Infosecurity Europe

Wick Hill Ltd will demonstrate at Infosecurity Europe how easy it is to hack into phone systems and carry out damaging attacks. Chairman Ian Kilpatrick says the problem is so large due to a lack of awareness about the risks. People are “still playing catch-up” when it comes to this type of security. “Some PBX vendors even deny there’s a problem, and claim everything is safe.” Threats include toll fraud, where calls are channeled through a PBX to premium numbers and hijacking PBXs so criminals can sell on minutes for profit.

Additionally, he says, “If I can break into your phone systems, there will be a bridge to the data network. That bridge is behind the firewall and is typically undefended. It is not perceived as risky. The biggest problem at the moment is the lack of awareness of the problem, as with all security. This is real; it’s not a hypothetical threat. We are trying to educate the market, and show the issues around the threats”

19 April 2011

Furness Firm Hacked by Somalian Phreakers

Optech Fibres, in the business of internet and telephone networks, were horrified to discover that their phone system had been hijacked to make hundreds of pounds worth of fraudulent calls to Somalia. Optical and IT Services manager Lance Jobson said, “The worrying thing is, if we, as a company which was aware of the scam, fell foul, so many others who know nothing about it could do too, so we want to raise awareness and warn other small businesses”. However, a spokesman for BT confirmed customers would be responsible for any fraudulent calls on their bill.

14 April 2011

Spate of Toll Fraud in Fredericton, Canada

Local police are warning residents that there have been attempts to steal long-distance calls – toll fraud – from homes and businesses in the area. “Members of the public or businesses may not realize they have been a victim until they receive their telephone bill” say police. This type of fraud takes in around \$12 billion a year.

13 April 2011

ITSPA Launches Best Current Practice Guide

“The purpose of this BCP by the ITSPA Security sub-committee, is to ensure best practice, gained from extensive experience across the industry, which can dramatically reduce the technical vulnerabilities and economic exposure on operators and end-users alike from the increasing fraud and hacking activity.”

[Control Phreak protects SIP (VOIP) lines as easily as ISDN or PSTN lines.]

12 April 2011

Perth Firms Hacked (also [here](#) and [here](#))

Hackers have targeted business in Western Australia, say police, after three businesses suffered losses of AU\$70,000. Calls were made to international numbers offering premium voice services – this is how hackers fund their illegal operations, including terrorism. They often own these premium numbers. Local police said, “As these criminals are working overseas and using quite elaborate methods to avoid detection, Western Australia Police find it difficult to identify or prosecute the persons responsible.”

1 April 2011

Phreakers are back, and in a Big Way

Over the last two years telecom security researchers have reported a very sharp rise in attacks against unsecured VoIP systems.

“The Phone Phreakers are back. But in the age of IP communications, they can target systems in any country in the world, and exploit weak security in any company’s telecom systems if they are not properly protected... Law enforcement authorities and fraud prevention groups in 2009 and 2010 described a sharp rise in toll fraud attacks, costing enterprises into the billions of dollars... IT trade journals and local media routinely report small companies receiving surprise long distance or charge call bills ranging from \$10,000 to \$100,000 or more. For a small business, such a bill can be crippling, and there typically is no way for the business to prove that these calls were not made by its employees... Industry researchers say that 1 in 4 hacking attacks utilizing the Internet are targeting VoIP systems and looking for improperly secured SIP trunks. Because the security safeguards at many companies have plugged the traditional hacking vectors, attackers have turned their attention to VoIP and SIP trunk vectors that are less well protected.”

9 March 2011

Hackers May Be Using Botnets, Cloud Computing

“A spike in attacks against IP PBXs that started last fall shows no signs of abating, spawning speculation that those responsible have tapped into botnets and cloud computing resources to carry out their illegal activities. Regulation: VoIP and compliance regulations make strange and difficult bedfellows.”

According to security reports from Cisco and Viper Lab, “the exploits are carried out using techniques that lend themselves to the interpretation that the attackers are tapping into broad resources that make their work more effective... The most common exploit against compromised PBXs is toll fraud - using someone else's phone system to make long-distance calls. The second is forcing the PBX to call premium numbers controlled by the attackers that charge by the minute. Businesses whose PBXs have been attacked are billed.”

3 March 2011

CA\$10,000 Shocking Hacking Bill for Small Business

Bob Pritchard, a home radio station owner from Saint John, New Brunswick, Canada was shocked to discover his PBX was being hacked – and the resulting bill was almost CA\$10,000. He noticed his phone lines were lighting up even when he wasn’t using them, but upon proactively contacting his telco to ask if he was being hacked he was erroneously told that they had been informed by the PBX manufacturer that “No, it’s simply not possible”, and that they were unable to check on the problem until his bill had been processed. This was of course untrue, and not only did the hackers continue to make illegal calls to North Africa in the weeks until the bill was processed, but once the telco confirmed that he had in fact been hacked, they expected him to pay. Says Pritchard of his unconcerned telco, “They said that’s my problem”.

Pritchard’s telco only backed down when he threatened to go to the police. “We had done due diligence. We had brought it to their attention,” he said. “If you bill me, and come back at me, I’m going to go back to the police and refer criminal charges against you for robbing me. Once I explained that to them, I got a whole different attitude. You take money from me, that’s stealing from me; you’re one of the bad guys.”

While Pritchard’s stance toward his telco had the desired effect, he remains concerned that other small businesses may be affected in the same way.

Canadian police say they will not become involved in disputes over who is liable for hacking costs, when telcos expect customers to pay up: “That’s all civil, it’s not part of the criminal investigation at all.”

22 Feb 2011

Businesses Hacked in Harrogate, UK

The average amount companies are hit for in such cases is £10,000 but one of these companies was phreaked for £25,000 over the New Year weekend. Phreakers prefer after hours, weekends, and bank holidays to aid in avoiding detection. Companies can set longer passwords and audit, but “as fast as these measures close one door, the hackers find ways to open another.” [Control Phreak is the only secure software option on the market.]

16 Feb 2011

PBX Hacking Threat Continues, Says Nimans

The CFAA now places the UK in one of the top five positions in the world as a “phreaking hotspot”. Nimans’ Dealer Sales Manager Tom Maxwell says that phreaking is underestimated by resellers and customers alike, and that resellers with their heads in the sand risk seriously damaging their business; resellers often end up blamed by customers for supplying an insecure system when these customers are phreaked, and often the resellers end up paying financial compensation. He says, “In most cases, they have also lost the customer as well! Bear in mind, the average cost to a victim of a UK Phreaking attack is currently estimated at £10,000. These are highly organised criminal gangs with state-of-the-art equipment which they use to hook chains of compromised PBX’s together to form their own networks” Nimans recommends Control Phreak, which uses Active Voice Security and has Panasonic’s global accreditation.

Maxwell says, “Ignore this threat and you could find yourself seriously out of pocket or damaging your business and its reputation. No company is immune from this growing menace.”

11 Feb 2011

Two Guernsey Firms Phreaked for £28,000 during One Weekend

The firms, in the finance and law sectors, had their phone systems hacked over a Saturday and Sunday, with illegal calls being made to places like North Korea and Somalia. DS Andy Whitton of the Commercial Fraud Department of the Guernsey Police said that “they dial the company and look for weakness and try to get in” and that these criminals were able to make calls to all over the world.

Update 14 Feb: one of these firms was subject to a second phreaking attack only days later. Guernsey Police warn other companies to take care to protect their phone systems.

11 Feb 2011

Taiwan Criticises Philippines over Cross-Border Telecoms Fraud Case

Taiwan’s Criminal Investigation Bureau (CIB) said Philippine law enforcement authorities arbitrarily released 17 Taiwanese suspects in a cross-border telecom fraud case they jointly busted on 22 December 2010. It said the Philippine authorities did not even complete a record of the questioning of the 18 arrested Taiwanese suspects before letting them go.

8 Feb 2011

Ireland's Department of Finance and Personnel Hacked by Phreakers [[video](#) about this news item]

The department's phone network was compromised by phone hackers. They contacted British Telecom with their suspicions about 18 months ago and the BT confirmed the phone network had been compromised. BT refunded the total cost of £34,000 and said it was putting measures in place to try to stop similar attacks in future. Dr Kevin Curran, a computer science expert from University of Ulster, said that many businesses and public sector bodies have been the victim of the similar scams, including Scotland Yard. However, because of cost and difficulties in trans-national law enforcement, telecommunications companies do not normally contact police about such scams.

8 Feb 2011

BBC PSA About Phreaking

Notes that phone hackers are sophisticated, employing teams of people and often taking advantage of weekends and bank holidays to avoid detection, and that PBX hacking is a multi-million pound crime annually in the UK alone. Dr Curran says that "anyone who underestimates the risk should be aware of one of the most high-profile victims from which hackers netted millions – New Scotland Yard."

3 Feb 2011

Long Distance Fraud a Problem in France

While France Telecom had problems with its own employees making fraudulent calls which were charged to third parties, the biggest problem is professional PBX hackers, or phreakers. Many companies are unaware that their PBX can serve as a springboard for criminals to make illegal long distance calls. Though often forgotten in the fight against technology piracy, PBX hacking is growing exponentially and causes incalculable harm. An unprotected PBX is "open to all attacks."

1-2 Feb 2011

Spate of Long-Distance Fraud in Bermuda ([update here](#))

Bermuda residents are being warned of recent toll fraud, where criminals have been hacking into PBX systems and making large numbers of unauthorised long-distance calls. This also happened in Bermuda in April 2009. The sums of money being lost through these illegal calls are "considerable".

24 Jan 2011

Sharp Increase in French Phone Hacking

Hacking has sharply increased within the last few months, says Guy Têtu, managing director of SSTR (Sociétés de Services en Téléphonie et Réseaux). For months the members of SSTR have been calling wanting to know solutions to protect their customers from phone fraud – to protect themselves from liability for this hacking.

One company's phone bill that was usually €1,000 became €24,000 due to illegal calls. Another company in the Paris region was phreaked in one week for €60,000, and a third company in the PACA region was left with thousands of Euros in extra charges after hundreds of hacked calls – each only around 20 seconds in duration – were made to the Balkans.

Claude Madar, CEO of Intellicom, has seen many of his customers hacked; one for €60,000, another for €14,000. Michel Matillon, head of the TSA, has had many cases reported to him. Some attacks had taken place in the holidays, with illegal calls made to locations in Africa.

Yoann Thomas, technical director of OpenIP – a SIP trunking operator whose customers have been phreaked – says that “statistically there are 300,000 attempted attacks in SIP or TDM (on the PBX) per year in France. This happens very often on weekends.”

10 Jan 2011

Heads in the Sand over Phone Hacking

Despite being a \$72-80 billion (annually) problem according to the CFCA (of which subscription/ID theft \$22 billion, compromised PBX voicemail systems \$15 billion, premium rate service fraud \$4.5 billion) awareness of this fraud remains minimal and resellers don't fully understand their responsibility to their customers concerning network security; in fact, around 90% of them don't. What is most worrying is that this ignorance serves the criminals – the more money they make perpetuating this fraud, the more they can invest in increasing their illegal activities. Customers, expecting a duty of care from resellers that is not being delivered, will hold resellers responsible and resellers are missing out on vital profit opportunities and strengthened business relationships if they don't add security options – like Callista's **Control Phreak** – to their portfolio.

Says Ian Kilpatrick, Chairman of distributor Wick Hill, “The extent of this problem is not fully quantified because it's in nobody's interest to admit that they're vulnerable. The perpetrators don't want to be found out, and **the victims are either unaware of the source of the information leakage, or if they become aware of it, they simply don't want their problems and security failings to be publicised...** Most people conceal any problems they have with [toll fraud]. In the channel, there's little discussion about the nature and size of toll fraud in the UK. The only toll fraud statistics available are global figures. This is despite the fact that the channel and many of the carriers are aware of how much toll fraud affects them. **There is information, but nobody wants it given out because nobody wants to be responsible for it.**”

4 Jan 2011

Comms Dealer Poll Shows Growing PBX Hacking Damage

62% of voters have customers who are the victims of PBX hacking, and 25% reported more than 20 cases within their customer base. Richard Winterburn, Strategic Partner Manager at Retell, said it was "incredible" that so many resellers and customers think their PBX is immune to hacking. He said, "I doubt any [phone] system is fraud proof. It's usually just a matter of time before hackers gain access one way or another."

Tom Maxwell, Dealer Sales Director at Nimans, also believes that telecoms fraud is a growing problem and needs to be at the forefront of channel debate this year. He says, "When you see the numbers involved on a global scale it's frightening. Everyone knows they need PC protection when surfing the web. It's the same with telephone systems."

Jack Wraith MBE, CEO and Director of The Telecommunications United Kingdom Fraud Forum (TUFF), believes that the highest levels of protection are necessary for people's phone systems. He says, "SMEs are particularly at risk from telephone hackers whose activities can cost the business many thousands of pounds. Hacking telephone exchanges that are operated by small businesses, schools and the like still figure highly in the fraud that is committed against the telecommunications industry."

6 Dec 2010

Customers let down by Resellers over Security [video also at link]

Resellers are ignoring their responsibility to customers as 'trusted advisors' by not providing information and solutions to PBX hacking attacks, says Ian Kilpartick, Chairman of [Wick Hill](#). New surveys rank security as the main challenge to unified communications deployment, and Kilpatrick says that "you need to incorporate advice on convergence security, so that at the very least, you minimise your liability risk if something goes wrong." As toll fraud increases it becomes even more remiss for resellers to leave security left unsaid in the sales process. [Control Phreak is an easy-to-use low cost solution to this problem, providing a real time solution to toll fraud and allowing easy user customisation so legitimate call traffic is unaffected.]

3 Dec 2010

Resellers Not Savvy When it comes to Voice Security

[Additional link: [TMCnet](#)]

Wick Hill says that 90% of resellers selling PBX systems don't fully appreciate the security risks. Voice security "is in the same place as internet security was 10 to 15 years ago," says Paul Brewer, technology solutions director at Datapoint (partnered with Avaya). Criminals – often linked to organised crime and terrorism – are getting over £1b a year from phreaking, and can also gain backdoor access to IT systems.

3 Dec 2010

Lack of PBX Security Awareness Becoming Reseller Liability [press release]

Siobhan Gibbs, UK Sales Manager for Wick Hill, says of the lack of focus on PBX fraud, "Clients need to protect their VoIP activities every bit as much as they protect their data activities, if they're to prevent toll fraud. ***If resellers are aware of the issues of toll fraud and don't advise clients of the need for security, then when something goes wrong, guess who'll get the blame?***" Of Control Phreak, Gibbs said, "Control Phreak is a big improvement on what was available previously, as that involved monitoring retrospective alerts, effectively closing the stable door after the horse had bolted."

25 Nov 2010

Shocking Phone Bill for Toronto Music Chain

Long & McQuade, which runs 50 stores across Canada, was hit with a \$83,000 phone bill after phreakers hacked their PBX. Steve Long, company president, says their telco provider Telus reduced the bill to \$25,000 but he is still angry he is expected to pay and the dispute has been ongoing for 18 months. Telus says that as Long & McQuade's PBX was compromised by hackers, Telus is not responsible for these charges and the music company must pay up. Telus' spokesperson Jim Johannsson said, "The PBX was hacked, *it was someone else's equipment so we're under no obligation to reimburse*. As a goodwill gesture, we do want to keep this customer's business, so we paid for some of the bill already."

Steve long is also demanding compensation for resulting lack of productivity, and is considering suing Telus and he feels they were never upfront about the risks of phreaking and how it works.

23 Nov 2010

Looking for Forum Advice on Long Distance Hacking

A member of Tek-Tips Forums reports that they have a client whose system was hacked. They were phreaked with international calling and 1010 numbers. Their telco AT&T had blocked these calling options, and the forum member had blocked "every remote access to outdialing" they could think of, including blocking the voice mail ports from dialing anything. However their customer's system was still getting phreaked.

16 Nov 2010

Volunteer Group Hit with £4,000 Toll Fraud Bill

The phone lines of the Flintshire Local Voluntary Council were used to make illegal calls to numbers in Africa, and also to premium rate lines. The group, a support organisation for 1,000 community and voluntary groups in Wales, is attempting to talk to their telco about avoiding paying the shock bill.

29 Oct 2010

Company Hit with \$100,000 Fraudulent Phone Bill

"Last week, my company got a \$100,000 phone bill. Turns out, some enterprising types have been bouncing their calls off our voice network. This allowed them to make numerous calls to a foreign country using our equipment. And it looks like we're stuck with the bill... Because our device is actually making the phone calls, the liability for the cost is ours."

19 Oct 2010

Lancashire Firms Warned of Toll Fraud

Local police are urging businesses across the Garstang and Longridge area to protect themselves against toll fraud that can leave companies facing massive telephone bills. The warning came after a doctors' surgery was left with a bill totalling several thousand pounds after their phone system was hacked into by criminals in Portugal.

11 Oct 2010

ComReg Ireland Warns of Rising Rates in Telephony Fraud

The Commission for Communications Regulation in Ireland warns there has been a number of recent attacks and advises businesses that they are responsible for their PABX's security, and if phreaked will likely face bills many times their usual charges – often up to tens of thousands of Euros. These fraudulent calls are usually not detected for some time. Businesses are advised to tell their telco providers immediately about these security concerns, and that if they are phreaked it is a matter for police.

6 Oct 2010

Panasonic Partners with Callista to Combat PBX Hacking

Panasonic Systems Network Europe and The Callista Group are working together to address phreaking. **Control Phreak** will be integrated into Panasonic's TDE and NCP voice switch platforms – the company's main PBX systems – providing complete security from phreakers.

Steve Gerrard, Marketing Manager at Panasonic UK, says that "It's not enough to know that an attack has happened and a crime committed. *By that time it's too late and the damage has been done...* incorporating Control Phreak means that users won't have to manually monitor retrospective alerts. They won't have to monitor anything."

He continues, saying that "**Switch hacking and toll fraud is a real and present danger that thrives on the lack of understanding within the market.** In partnering with Callista, **Panasonic is taking a positive stance against this type of crime** and further securing our intelligent voice solutions for the benefit of our customers... We have been pioneering this anti-phreaking solution with Callista in other parts of the world, now we are in a position to offer this secure communications solution to UK customers."

August-October 2010

UK's Business First Magazine Phreaked During Summer Break (Online magazine article, p14-17)

Illegal calls were made from Business First Magazine's PBX to North Korea, and as a result of this criminal attack the company has been forced to change their business phone number. Business First Magazine's telco British Telecom did not have a policy of informing customers of unusual call patterns (as many do), so the magazine has changed teleco providers. The phone bill was several times its usual amount and the attack happened over the summer holidays when the office was closed. BT's response was to say that it was not their responsibility, and that Business First Magazine should have been using passwords and was completely liable, even though passwords are not effective against phreakers. Similarly, insurance is no guarantee – most policies classify this hacking as 'electronic losses', which are exempt. The police are extremely unlikely to be able to do anything as phreakers are usually international criminal gangs expert in distancing themselves from the attacks. Business First Magazine discovered that Callista's Control Phreak is the only software-based PABX firewall on the market.

27 Aug 2010

Swedish Small Business Phreaked for Kr 95,000 in One Week

Phone-fraud criminals hacked the phone system of VINATOR Chefsrekrytering (VINATOR Executive Recruitment) to the tune of Kr 95,000, the fraud taking the form of 1,400 illegal calls made at night, after business hours, to Somalia. A small company, VINATOR's usual phone bill is Kr 1,500 per month. They were also phreaked in the summer of 2008 but in this case the attack triggered their telco supplier Tele2's unusual call alarm after Kr 20,000. Mikael Höstman, technical manager for Panasonic Nordic, believes the phreakers likely used an automated password cracking program. This can reduce password hacking to mere milliseconds. Panasonic recommends Callista's Control Phreak firewall system for constant monitoring and superior PABX safety.

19 Aug 2010

Phone Fraud Criminals Hacking NZ Firms (also [here](#))

About 40 NZ companies a month are being hacked by international criminals, up to \$50,000 a time for some. The Telecommunications Industry Group says that "New Zealand companies [are] losing hundreds of thousands of dollars annually through this fraud, which [has] increased fourfold this year." TIG says that it is "big crime" that in the US costs US\$4 billion annually and that "the average level of loss [in NZ] is about \$10,000 per event". **Hacked businesses are liable for the charges because local telco providers have to pay the international telcos where the calls have been placed, and do not want to be out of pocket themselves.** Recommends passwords etc, but this is not protection against phreaking as even multi-digit passwords can be hacked in milliseconds by modern password cracking programs easily available on the internet. "The first quarter of this year has seen a 400% increase in phone fraud", says TIG, and this is affecting more and more small businesses.

9 Aug 2010

UK Tech Supplier BCL Phreaked for over £10,000 in Just Four Days

Insurance company declined to pay out, claiming it was BCL's responsibility. Police knew of similar cases but said tracking the criminals was unlikely. BCL had to pay half the bill in order to keep use of their phone system and had to disable outbound international calls entirely, with their voicemail ports only protected with passwords which they knew would not work – until they started using Control Phreak. BCL believes many businesses do not realise how vulnerable they are to attack – they did not. *"I would urge any business worried about their telephone security to invest in Control Phreak. For the sake of a few hundred pounds it can save you a fortune and bring total protection."*

6 April 2010

Phone Hackers Target New Zealand Firms

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".

11 Mar 2010

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

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

11 Mar 2010

UK in top 5 for Global Communications Fraud, says CFCA

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.

23 Feb 2010

Adelaide Business Defrauded of Up To AU\$100,000

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

8 Feb 2010

98% of Hackers also Hit Businesses with Dial-through Fraud

Phone hackers love long holidays and many businesses come back from the Christmas / New Year break to a nasty and expensive PBX hacking surprise, as criminals exploit the lowered call traffic monitoring over these holiday periods. This telephony crime has grown during the economic downturn. According to [Telecommunications United Kingdom Fraud Forum \(TUFF\)](#), when they surveyed their membership in late 2009 comms and service providers reported that *98% of businesses that were hit by hackers also suffered from dial through fraud*. TUFF believes that many companies are unaware that DTF could happen to them and are still not doing enough – or anything – to protect their assets. Bills could be as large as £95,000 in a short period of time.

29 Jan 2010

\$24,000+ Long Distance Fraud

A forum member seeks advice on how to possibly get their customer's telco to zero all charges after they were phreaked for over CA\$24,000 in overseas calls afterhours on Christmas eve. Other forum members respond that because telcos consider the problem of phreaking to be due to insecure equipment, telcos generally do not assume responsibility and thus the phreaking victim is liable for the charges. One forum member who works for a telco says that they occasionally lower charges on compassionate grounds, but do not generally zero them. "What's happened is that an insane amount of volume (24,000+ minutes) was done using only three phone lines, in a 14.5 hour window. Dozens of simultaneous phone calls... on only three lines."

1 Dec 2009

PBX Fraud Strikes Toronto

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).

27 Oct 2009

Internet Phone Systems Become the Fraudster's Tool

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.

2 Sept 2009

Toll Free PBX Hack Highlights Need for Increased Security

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.

Late 2009

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.

24 Aug 2009

Gamma Telecom Aids PBX Resellers' Fight against Telephony Fraud

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.

(No date, ongoing)

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.

30 June 2009

Notorious Phreaker Gets Sentenced to Eleven Years in Prison

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.

13 June 2009

Hacking-Terror Effort Thwarted

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.

June 2009

International Phone Fraud Ring Busted

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.

June 2009

PBX Hacking Moves into the Professional Domain as Arrests Stack Up

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.

13 May 2009

Irish Department of Social Affairs Phreaked for €300,000. €12,000 in One Weekend Alone

A European police department was hacked for £1m sterling over six months. US mobile operator Omnipoint defrauded of US\$9.6m and as a result "75% of the company's market capitalisation was wiped off, despite it having upwards of 200% customer growth."

"Telecoms fraud, or technically private branch exchange (PBX) fraud, is one of the most prevalent, yet under-publicised, forms of computer fraud around. IDC estimates there are more than 200 variants of the fraud in operation... [and it] currently accounts for between 30% and 50% of European telecom firms' bad debts."

29 Jan 2009

Significant Increase in Irish Telecoms Fraud Threatens Cash-Strapped Businesses [also [here](#)]

A rising number of Irish companies are being targeted, with this type of crime costing Ireland millions of Euro annually. Costs to businesses vary depending on the case in question, but the scam can cost a business thousands of euro. In Ireland, the Garda Bureau of Fraud Investigation ([which recognises telecoms fraud as a serious problem](#)) estimates that telecoms fraud can be as high as €90,000 over just one weekend. Outside hackers and 'time theft' has grown to unacceptable proportions according to MinuteBuyer's market intelligence." Says Shaun Hayden, Director of MinuteBuyer, "The economic downturn has, it seems, brought with it an increase in opportunistic time theft and fraud... The time-theft costs are particularly tough on smaller SMEs, which cannot absorb the costs the way larger companies can."

27 Jan 2009

Bell Canada Customer Billed \$207,000 after Hacker Breach

Toronto businesses angry that they have 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 is not) and says that passwords will offer adequate protection (they do not, as the phreaked businesses point out in the article).

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

(Has associated CBC News video on right-hand side of the linked page).

22 Jan 2009

Phreakers Hit Australian Companies

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.

12 Jan 2009

Suing for Poor Performance

Charles Cockburn, lobbyist and chairman of [Portcullis Public Affairs](#), was the victim of dial-through fraud for £22,000 and 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.

01 Jan 2009

Firms Face Rise in Phone Fraud

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

(No date, ongoing)

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.

22 Dec 2008

Voicemail Hack Costs Business Owner \$43,000

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.

20 Aug 2008

US Department of Homeland Security Subject of PBX Hacking

FEMA (part of the US Department of Homeland Security) was defrauded by just one hacker for US\$12,000 through their PBX, with illegal calls being made to Afghanistan, Saudi Arabia and Yemen, among others. The hacker made over 400 calls.

29 July 2008

Telecom Frauds Not Taken Seriously by Companies

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

19 April 2007

Nortel PABX Hacked Again

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”.

17 Oct 2006

Telephone Hack Costs NSW Firm AU\$9,000

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 do not want to admit to being phreaked out of embarrassment over security.

8 June 2006

Feds Arrest VoIP Exec for Wire Fraud, Computer Hacking

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.

23 Nov 2005

Phreakin' Hell: Phone Hacking Costing Australia Millions

Phreaking costs some companies up to AU\$1 million in single attacks. Companies do not 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 do not discriminate between small and large business, and illegal charges can be enough to bankrupt.

16 Sept 2005

Telecoms Fraud Still Big Threat, Says Garda Bureau of Fraud Investigation (Ireland)

The head of Garda's Computer Crime Investigation Unit says that the problem has affected many Irish organizations and that "there have been lots of cases and the amounts of money collectively would come up to several million euro over the last few years... Companies should treat their PBX system in the same way as their computer network" Telecoms fraud is considered simple, profitable, and carrying little risk by criminals as while data security is now a prominent issue, telecoms fraud is still not taken seriously enough.

20 July 2004

Filipino Phone Phreakers Foiled

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.

Other evidence:

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).

A MinuteBuyer (Ireland) client **defrauded of €40,000**. World Trade Group (London) **phreaked for £27,000 over one weekend** (Enterprise Ireland, eBusiness Live, March 2009; reported directly to Callista 2008/9).

See also **Callista's video on phreaking and how Control Phreak can stop this global fraud problem.**

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
Bridge St | Stratford upon Avon | Warwickshire CV37 6AH | United Kingdom
Tel +44(0)1608 610025 | support.uk@callista.net | www.callista.net

Callista and Control Phreak are registered trademarks of The Callista Group Limited.
Copyright © 2012 The Callista Group Limited

