digitel
Business Communications

Telephone System Hacking Costs UK Businesses £1.2 billion Every Year

Normally we associate hacking with computers, not telephone systems. However, telephone system hacking and other telecommunications fraud costs the UK economy £1.2 billion every year. In today's business environment telephone system hacking, known as 'Phreaking', has seen a dramatic increase in activity over recent years, as can be demonstrated by the numerous newspaper, television and radio reports.

The reason we are experiencing this dramatic increase in telephone system hacking activity is simple. It's big business involving organised crime from around the world. These criminals use sophisticated equipment to attack telephone systems to use their trunk lines for their own purposes.

They use the hijacked lines to gain access to high cost telephone destinations and services throughout the world. They then resell the services to unsuspecting users who pay for the services provided by hacked telephone system, which of course they are using free of charge as you are paying the bill.

The vast majority of the hacking activity is primarily targeted at telephone system features like Direct Inward System Access (DISA) and Voicemail Access. If left unprotected these features can allow access to your telephone lines and services. Once the criminal has access to the services that is where they make their money.

It is important that these services and others that allow access to your telephone system are protected with proper passwords. Simple patterns such as 123456 or 246810 are also easy to discover. Your telephone system needs to be given as much consideration as your computer system against malicious hacking.

Some examples of the costs to business of phreaking are given below.

In November 2011, a group of four phone hackers in Manila were arrested for allegedly trying to break into various telephone systems, including that of AT&T, at the behest of a Saudi-Arabian terrorist group.

The Philippines' Criminal Investigation and Detection Group (CIDG) made the arrests in co-ordination with the FBI, and in a statement said, "The hacking activity resulted in almost [US]$2 million in losses incurred by the company."

Closer to home, COMREG, Ireland's telecommunications regulation authority, saw an increase in complaints about phone hacking over the first half of 2011, most of the calls made outside office hours. The reported attacks alone cost Irish businesses 620,000 euros in the past two years.

In Febuary, one single incident in Guernsey cost two firms 28,000 pounds. The firms, in the finance and law sectors, were hacked over a weekend, and calls were made to countries such as North Korea and Somalia. One of the firms was then subjected to a second phreaking attack only a few days later, adding insult to injury.

The UK is now considered one of the world's top 'phreaking/hacking hot spots' in the world according to the latest research from The Communication Fraud Control Association, along with Cuba, the Philippines, Lichtenstein and India.

Small to medium businesses are targeted as they are most vulnerable, and the average cost to a victim of a UK phreaking attack is estimated at 10,000 pounds.

digitel
Business Communications

Access methods used by Hackers

There are many methods of access used by the Hackers once their systems have access, they merely use the features of your telephone system to dial through to your lines and out onto the general network. This may sound simple however; there are quite complex systems involved.

The hackers generally network several hacked systems together, usually with complex dial through digit strings in-between systems, which can make it almost impossible to trace them. The profits are generated by dialling international and premium rate numbers and selling access onwards. The profits made from these illegal activities are in the hundreds of millions, and the cost of hacking can have a dramatic impact on any business.

For example if let's assume that one phone line can generate 4 pounds per minute in call charges. An attacker starts using your system at 17:31 on a Friday and is detected (and ceased) at 9:01 on the following Monday. This adds up to 3810 minutes of call time, which costs you 15,240 pounds!

If your system has fourteen lines, and the capability to generate an outgoing call on each, a hacker could set up seven dial-through calls, driving that figure goes up to a nightmare 106,680 pounds!

Even if we take a more conservative outlook and say the line only generates 1 pound per minute that still adds up to 26,670 pounds, which is an excellent return for a weekends work!

Minimise your risk

It is important to note that there are steps that you can take, however your telephone system maintenance provider should be consulted as your system may require reprogramming. They can also provide you with the assurance that your telephone system is as protected as it can be.

It is important to note that older systems can be more vulnerable than the more modern systems on the market today. Finally, while it is possible for an audit to identify and minimise the risks to a very low level, no set of actions can absolutely guarantee your system security against hackers.

- Do not leave passwords to your staff. Implement a company password procedure and develop authorised passwords. Distribute them out to staff and change them regularly.
- It is important to remove all manufacturer's default passwords and do not use default passwords, passwords like 123456 or ones generally known throughout the business.
- You should not use telephone extension numbers as passwords.
- Passwords should not be based on based on simple number combinations (e.g. 0000, 1111 or 121212).
- Passwords that use patterns (123456 or dial pad patterns such as 147852 should be avoided).
- Make sure you program your voicemail system to require passwords with a minimum of at least 6 characters, more if possible. Generally more characters means better protection.
- If possible disable all forms of automated trunk to trunk or automated straight through dialling which allows you to make telephone calls through your voice mailbox or telephone system (DISA) service from outside your company. If this feature is programmed into your system. It is important that you both monitor the service and generate reports to ensure your mailboxes or the DISA services are not being abused.
- Remove all unassigned telephone extensions or other unused services from the telephone system.
- Remove all unassigned voicemail boxes from the telephone system.

Digitel can perform a full security audit on your telephone system, or recommend improvements for both security and maximising your protection. Please contact our customer relations department for further information.