take command
COMMANDER

Protect your business from PABX FRAUD

Important information on Telecoms Hacking.

Reduce the risk of fraud through your communications services.

What to look for.

Some of the warning signs that your systems security has been compromised include:

- Large call volumes at night, weekends or public holidays;
- IDD calls to destinations you usually don't dial;
- An unusually high number of short duration calls;
- Difficulties (busy or delays) with retrieving Voicemail messages.

The cost of not securing your phone system

Hacking and fraudulent use results in unauthorised call charges billing directly to your account, as a business you are responsible for maintaining the security of your hardware. You will be liable for all charges incurred on your account. For further assistance contact your phone system maintainer or administrator to help minimise the risk of hacking.

Anyone with a communications system, either premises based PABX or a Hosted Phone System is a risk. The following examples highlight the need to improve your systems security.

Case Study 1

A large business facilities provider with PABX was attacked by fraudsters.

Lack of password security provided the hackers with free access to channel IDD calls through their PABX. The system maintainer was called when voicemail messages could not be retrieved. By that time the fraudsters had made over $80,000 worth of international traffic in little less than a week.

Case Study 2

A medium sized consulting firm with a Hosted Phone System was recently a hacking victim.

The provider noticed an abnormally large number of international calls and notified the customer. Security measures were put in place to prevent further calls, however, over $30,000 worth of IDD calls to Sierra Leone had already been made.

It's your responsibility to ensure the security of your communications system, failure to take security precautions could cost you a large amount.

Background

Telecoms hacking is communication fraud and can be defined as the use of telecommunications products or services with no intention of payment.

This industry-wide problem has increased in recent years, impacting businesses that own or operate PABX's, Voice Mail Systems or Hosted Phone systems. Fraudsters gain access undetected and make outbound calls both domestically and internationally resulting in substantial unauthorised costs being incurred by your company.

How does it happen?

Hackers gain unauthorised access to a customer's PABX, Voice Mail Systems or Hosted Phone system.

A hacker can compromise unprotected telecommunication equipment by dialing or logging in remotely to gain access to your communications system. Hackers usually exploit poorly secured remote access options such as Voicemail, or DISA (Direct Inward System Access) and once having gained access, redirect calls to anywhere in the world.

The fraudster may then masquerade as a service provider offering international access, or often generate large volumes of calls to their own Premium services. The hacker generates revenue using assets, resulting in substantial charges to your company.

> *"Hackers usually exploit poorly secured remote access options such as Voicemail...*

Your obligations

As the Service Owner, you are responsible for the administration and security of your Phone System.

This includes both physical security of PABX and Handsets, as well as Passwords and PINs used for remote access to premises based equipment of Hosted Phone Systems.

In some circumstances, we may become aware of possible Systems hacking or fraud, and as a matter of courtesy, provide you with notification, however we will only be aware after the fraud has been committed.

No responsibility will be taken by Commander where your system security has been breached. You will be required to pay for any charges generated as a result.

What action can be taken to reduce the risk of fraud?

Protecting your business assets from fraudulent use is best determined in consultation with your systems maintainer or administrator.

Commander recommends that your systems security regime includes the following measures:

1. Change default codes and passwords immediately once a service is activated.
2. Don't choose obvious passwords i.e. extension number, 1234, Company name.
3. Educate your staff on the importance of keeping codes and passwords confidential.
4. Enforce company policy to regularly change PINs and passwords.
5. Limit the number of employees with authorisation to set up new codes and passwords.
6. When a member of staff leaves the company cancel their access rights.
7. The External Call Forwarding feature of the Voice Mail System should be disabled, unless specifically required by staff member.
8. Disable any feature not in use that may be accessed remotely.
9. Delete any voice mailbox services that are not required.
10. Only authorised personnel should have access to the phone system equipment.
11. Keep phone system hardware in a secure place with restricted access.
12. Ensure you have adequate barring levels placed on your phone system, for example bar 1900 calls or international calls.
13. If your PABX has DISA enabled (Direct Inward System Access), then only limited specific staff should have access to that feature.
14. Unused extensions should have their access rights deactivated.
15. Check your phone bill for any unusual call traffic.