PABX AND VOICEMAIL FRAUD

This industry-wide problem is increasingly impacting businesses that own or operate Customer Premises Equipment (CPE), typically PABX or voicemail systems, which fraudsters can access and make outbound calls domestically or internationally.

Many fraudsters know how to access your company or employee's voicemail services and use these to make domestic or international tolls billed to your account.

The costs associated with CPE fraud escalate very quickly and can amount to tens of thousands of dollars, especially if the fraudster is selling calls for profit but billing them to your business.

How are the fraudulent calls made?

The problem occurs when an automatic voicemail system (or similar) that allows incoming callers to dial extensions directly or dial outside lines, doesn't have appropriate security measures in place. As a result hackers are then able to make a large volume of international calls that are charged to the customer's account.

Minimising your risk

It is vital you check your PABX system is secure as soon as possible. We've compiled some prevention strategies below to help you secure your system.

If you want to be sure you have the correct security configurations in place, you may wish to arrange for a Telesmart to visit your premises (normal call out charges will apply). Or if another provider maintains your phone system, you may like to arrange for them to visit.

Will I have to pay for fraudulent calls?

You are responsible for ensuring appropriate security measures are in place, and therefore you are also responsible for any charges to your account resulting from inadequate security measures. Please ensure you take the necessary steps to ensure you're not at risk.

PREVENTION STRATEGIES

1. Never give out technical information about your system to callers - unless you are certain you know who you are talking to.
2. Do not allow your system administrator to maintain factory set passwords for maintenance of your system.
3. Get your PABX vendor to barr international and 0900 calls from your PABX's voicemail ports.
4. Introduce a PIN and password management policy where employees are not permitted to use predictable PIN numbers such as the last digits of their DDI, sequential numbers like 1111, or incremental numbers like 1234. Ensure that PIN numbers are changed regularly, and supervisor and maintenance passwords are changed when the administrator leaves.
5. Do not allow unlimited unsuccessful attempts to access your voicemail. Configure the system so that 3 unsuccessful attempts results in call failure to the voicemail number.
6. Disable an employee's voicemail number when s/he leaves your company.
7. If you do not need remote access to your PABX, then turn that functionality off. Or if support is outsourced, ask your vendor to do this for you.
8. Make sure your PABX room is locked when not attended.
9. Be alert to the overt signs of PABX fraud such as repeated calls of short duration, high numbers of inbound hang-up calls, unexplained increases in incoming calls where the caller hangs-up when answered, sudden increases in 0800 usage, difficulty obtaining an 'outside line', or changes in after-hours calling patterns. This can be monitored through your PABX logging/reporting service, which enables you to view daily usage.
10. Make sure you understand the terms and conditions in your contracts with your PABX, VoIP and/or voicemail vendor in regards to keeping your system regularly maintained and serviced to stay safe.

Telesmart
TAILORED NETWORK, VOICE & VIDEO

iua