VIDEOTRON | BUSINESS SOLUTIONS

IMPORTANT: TELECOM FRAUD PREVENTION (REMOTE PBX INTRUSION)

Dear Customer:

In response to an increase in PBX telephone system fraud within Canadian businesses, we wish to help raise awareness in regards to the infiltration methods used by many fraudsters and inform you of the main repercussion of telephone fraud. We would also like to take this opportunity to remind you of the recommended security measures when it comes to telephone system configuration.

HOW A TELEPHONE SYSTEM OPERATES

A PBX is a telephone system that allows companies to manage internal and external communications. Telephone systems function the same way as computer servers used conjointly with known operating systems, but they're equipped with a telephone application. Security wise, telephone systems are subject to the same constraints as computer servers.

HOW DO FRAUDSTERS INFILTRATE THE SYSTEM?

Fraudsters generally access your telephone system by using diverse techniques to guess your voicemail passwords. Once the system is accessed from outside your business, telephone hackers use it to reroute calls to outside the country. In fact, hackers often reroute calls abroad, to countries where the per-minute calling rate is extremely high. Fraudsters generally hack into telephone systems at night, on weekends or during holidays, hoping that their infiltration goes undetected. It is important to remember that IP telephone systems connected to the Internet can also be targets of fraud.

THE MAIN REPERCUSSION OF TELEPHONE FRAUD: OVERBILLING

Overbilling as a result of numerous overseas long-distance calls is the main repercussion faced by a business when it becomes a victim of telephone fraud. It's important to reiterate that you are responsible for any costs associated with calls placed or received on your phone line (i.e.: collect calls), regardless of whether you have taken reasonable security measures in the fight against fraud. Telephone fraud is a crime. If you think you are a victim of fraud, we suggest you contact your local authorities immediately.

HOW TO LOWER THE RISK OF FRAUD

Here are a few recommended security measures you can take to help protect your telephone system. This list is not exhaustive and is intended for information purposes only.

- Avoid obvious passwords, such as phone numbers, extensions, simple sequences (12345678) and consecutive or repetitive numbers (00000000).
- Immediately change the default passwords provided with the installation of new equipment or the creation of voice mailboxes.
- Regularly change your passwords (i.e.: every 60 days).
- Remove or restrict unnecessary features, such as those that allow calls to be made to outside the country: Conference Calling, calls made from your voicemail system, the use of telephone operator services (0+), etc.
- Limit access to the telephone system to authorized personnel only, even during business hours or holidays.
- Never publish telephone numbers that could provide direct access to the system (Direct System Access, DISA).

- Limit or block outgoing calls outside of business hours.
- Disable all inactive mailboxes.
- Ask your telephone system provider to regularly update your equipment.
- Regularly audit your telephone system in order to re-examine its configuration and level of security.
- Encourage your employees to adopt sound practices by adding telephone system security to your information security policy.
- Install a firewall to filter incoming IP addresses.
- Subscribe to an insurance policy against financial loss caused by telephone fraud.

TALK TO YOUR TELEPHONE EQUIPMENT PROVIDER

Remember that you are responsible for protecting your telephone equipment. Ask your provider, who ensures the support and management of your equipment, to apply adequate security configurations and norms.

We hope that these tips will help you better protect your business against telephone fraud.

*Please note that Videotron is not a provider of telephone equipement and that the content of this letter is provided for information purposes only.