January 2013 – Information Received from the Channel Partner Department

Approximately 13 Shaw Business customers, primarily in Kelowna, have been targets of Toll Fraud over the past two weekends. The perpetrator(s) have been sniffing entire ranges of IP addresses (Kelowna) attempting to detect VoIP servers. Once a response is returned indicating a VoIP service, they then "brute force" attack the IP looking for weaknesses and/or easy passwords, most likely voice mail (VM) boxes, or IP phones. This is most likely what is happening, although only the third party vendor, who installed or manages their VoIP server will be able to determine that after completing a comprehensive audit. Once a VM box or IP phone is compromised, the hacker will log in as that user and begin making international long distance (ILD) calls or calls to the Caribbean Islands.

To protect Shaw customers, we do have a process and it is very similar to other ILECS/CLECS. The following is the process and the events that transpired:

- Shaw Telephony Investigations were alerted to unusual or high cost calling patterns,
- Customers were contacted, but in most cases voice messages were left due to after hours. The contact number of the Shaw Telephony Investigations Team was provided.
- ILD and/or LD feature was disabled. Usually within four hours, depending on technical or resource issues,
- Customers were spoken to by the Shaw Telephony Investigations Team the next business day and advised to contact their third party VoIP vendor to determine how the hacking occurred, and to contact Shaw billing to determine the actual amount they will be billed. Shaw usually only bills their costs to the customer, thereby reducing the invoice.
- The customer's ILD feature will remain disabled until a person of authority within their company requests to have it re-enabled. Usually after the vendor determines where the weakness is in the VoIP server and institutes security lock downs.

Please note that Shaw Telephony Investigations disabled ILD and/or LD on all targeted customers shortly after they were hacked, thereby saving them an enormous bill . Furthermore, while the Shaw Telephony Investigations Team does not provide information on billing reductions, the appropriate people within Shaw were notified, to speak to customers about that fact.

In situations where Shaw Business does not manage or host the VoIP PBX, the customer is ultimately responsible for all calls originating from their service or traversing their system. Third party vendors of VoIP Servers/PBXs have a "duty of due diligence" to ensure that all weaknesses are appropriately locked down. Of course, as new weaknesses are discovered, customers need to be proactive to ensure they take steps to mitigate the risks.

There is an entire industry that has evolved due VoIP hacking, sniffing, intercepting etc. Many third party vendors have recognized this fact and offer value added services such as VoIP security audits, firewalls particularly for VoIP, Session Border Controllers etc.

This problem is not going to go away anytime soon. Shaw will continue to protect its customers, and does what all similar service providers do. Unfortunately, it is usually after the fraud has been committed due to security weaknesses in customer provided equipment.

Shaw Business