Customer Alert - Protective Actions to Help Stop Toll Fraud

We have seen an increase in instances of Toll Fraud and this can have serious financial impact on your business.

Definition: A crime in which a hacker obtains telecommunication services by breaching computer security, accessing a PBX and using its communication facilities illegally. Toll Fraud is estimated to cost UK companies in excess of £1bn/year.

Toll Fraud Destinations: We have seen calls to premium rate numbers i.e. 09xxx, non-geographic numbers i.e. 0871, even 0844, mobile Wi-Fi numbers i.e. 07xxx as well as international destinations.

Toll fraud usually occurs outside business hours when the activity is unlikely to be noticed. Fraudsters can make huge amounts of calls, often running up bills of thousands of pounds per trunk per day until stopped and because your carrier has provided its service legitimately, to you, they will charge for these calls. Therefore a bad case of toll fraud can have serious financial impact on a company.

A business break and bank holidays can increase the impact

There are some basic safety precautions that should be put in place by any customer using SIP devices, the Avaya PBX or Avaya voicemail. We cannot eliminate the potential for Toll Fraud. However, taking the steps outlined and carrying out any recommendations following a review will mitigate the impact.

1) If you have SIP devices (iPad, soft phone, mobile client, SIP phones etc.)
    - You must ensure that a 'strong' password is used – not the extension number or easy to guess passwords.
    - You should only use SIP devices if both the phone system and the SIP device have a mechanism to secure SIP (e.g. Digest Authentication)
    - Never expose SIP phones (softphones or hardphones) to the Internet without encryption or a VPN. Talk to Britannic if you need advice on how to secure remote devices.

    Additional recommended steps

    - If SIP endpoints are not being used then unchecking the "SIP Registrar Enable" option can increase security. This should be done for interfaces that have Internet access. Note that disabling this on both Interfaces (LAN1 and LAN2) will disable any SIP endpoint from registering with the IP Office.
    - Enable and use "User Rights" to control calling privileges. The Administrator can define limited calling as default rights of endpoints thus limiting calling to extension-to-extension and emergency only, for example.
    - Ensure that the IP Office is not connected to the Internet without substantial data security deployed. A Session Border Controller to limit SIP exploits is also recommended as stated above.
    - Ensure TCP/UDP ports are well managed at the Internet firewall and follow the guidelines for TCP/UDP port usage documented in the IP Office Knowledge Base.

2) Ensure that your individual voicemail box users have changed their passwords

- Examples of passcode to **not** use:
- 1234 Consecutive
- 123456 Consecutive
- 2580 TUI Pattern
- 159 TUI Pattern
- 0000 repeating
- 1435 if the extension is 1435 or 5341

3) Further Considerations:

- Changing to 6 digit passwords.
    - Note: The system will not allow the same digit to be used simultaneously (1111) or consecutive numbers (1234).

- Ensure the default of 3 wrong attempts to gain access to a voicemail box is enabled.
    - This locks out the user. (This must be reset by the administrator.)

- Invoke password ageing:
    - This will prompt your users to change their individual passwords upon first access of the mailbox and at pre-defined intervals (ie.3 months)

- Invoke call forwarding to specific users only.
    - Restricted by using a separate class of service.

- Invoke out-calling / remote call transfer to specific users only.
    - Restricted by class of service.

- DISA Remote-Access
    - Ensure barrier codes, maximum number of calls or end dates have been administered.

Request a 'Fraud Risk Assessment' to be carried out. There is currently a 10 day lead time, to be done on a first come, first served basis. There will be a nominal charge of £125.00 per system. We will remotely access your system to do the assessment.

The checks will include the following:

- Check system administration passwords and password ageing & notify you if found to be defaults.
- Check multiple user mailbox passwords at random.
- Review the switch setup in respect of barring, including trunk barring, remote access.
- If appropriate update barring policies – i.e. known current mobile Wi-Fi numbers, include in the barring tables.
- Advise on recommendations for additional programming if required, and any costs that may be associated.
- Advise the findings and what actions should be taken.

Further information can be located on Avaya's support website:
https://support.avaya.com/

AVAYA