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 and other premium rated 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 steps that must be taken by any customer using Mitel embedded voicemail or SIP devices as failure to do so may be seriously expensive. 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 clientetc.);-
    a. You must ensure that a strong password is used – not the extension number or easy to guess passwords.
    b. You should only use SIP devices if both the phone system and the SIP device have a mechanism to secure SIP (Digest Authentication etc.)
    c. Never expose SIP phones (softphones or hard phones) to the Internet without encryption or a VPN. Talk to Britannic if you need advice on how to secure remote devices.

2) Ensure that you change your mailbox passwords* on your voicemail platform; -
    a. Admin
    b. Manager

3) Ensure that your individual voicemail box users have changed their passwords*;-
    a. User default is 1111
    b. Don't forget the Operator mailbox

4) Further Considerations;-
    a. Changing to 6 digit passwords
    b. Invoking 3 wrong attempts to gain access to a voicemail box (software version 9.0 and above) – locks out the user. This must be reset byadministration.
    c. Only allow call forwarding to your 'speed dial' numbers – this means thatcallers that want to divert, for example to their mobile, will need their mobile number added to the speed dial table.

d. Request a 'Fraud Risk Assessment' be carried out (at time of writing there is a 10 day lead time – provided on a first come, first served basis). There will be a nominal charge of £100.00 per controller. We will remotely access your system to do the assessment. The checks include:
    i. Check system administration passwords (2)a. & 2)b. above) and change if found to be defaults.
    ii. Check multiple users' mailbox passwords at random.
    iii. Review the set ups in respect of barring, including trunk barring.
        1. If appropriate, update barring policies – i.e. known current fraud mobile Wi Fi numbers, include in the barring tables.
        2. Advise on recommendations for additional programming if required, and any costs that may be associated.
    iv. Advise the findings and what actions should be taken.

*The password needs to be something unique to the user, definitely not 1111, 1234 etc.