



Advice on preventing telephone fraud

GPC has been made aware that telephone systems used by practices may be vulnerable to fraudsters hacking into them and making premium rate calls. In one instance £2500 - £5000 of calls were placed over one weekend.

This is known as PBX/dial-through fraud, which occurs when hackers target Private Branch Exchanges (PBX) from the outside and use them to make a high volume of calls to premium rate or overseas numbers.

The victims are usually small to medium-sized businesses, but the National Fraud Intelligence Bureau has also noticed that a number of schools, charities and medical/dental practices being targeted where fraudsters are taking advantage of flaws in security systems.

This type of fraud is most likely to occur when organisations are most vulnerable i.e. during times when businesses are closed but their telephone systems are not, for example in the early hours of the morning or over a weekend or public holiday.

There are commercial organisations that will install software to prevent this and practices should consider whether this is a cost effective solution. However, a simpler alternative might be to place a block on international calls with the telephone system supplier.

This raises an issue of where, for example, a patient is hospitalised abroad and clinician to clinician communication is required, but the advice of GPC would be to ensure that an alternative mechanism for making and receiving such a call was in place, such as the mobile of one of the practice staff. Any cost to the individual could then be reimbursed.