



Just as unlocked doors offer open opportunities to thieves, unsecured Telephone System (PBX) systems offer open opportunities to telephone hackers.

Telephone fraud is on the increase, as Jack Waith, CEO of Telecommunications United Kingdom Fraud Forum (TUFF) states:

“ Hacking into small business exchanges has seen a rise in the past year and the level of this activity would indicate that small to medium businesses who operate their own office telephone exchanges are not securing their equipment against the activities of “hackers”. In many cases, this results in the small business having to pick up very large telephone bills from their communication providers. In a recent survey carried out one case of hacking resulted in a bill for £95,000. ”

How do hacks occur?

There are two types of hacks affecting PBX systems – Voicemail dial-through, and PBX dial-through fraud:

Voicemail dial-through fraud:

- A hacker dials a number and goes through to voicemail.
- The hacker enters the voicemail password.
- This gives the hacker access to an outside line.
- Hackers can then make calls through the PBX system, incurring call charges.

PBX dial-through fraud:

- PBXs are like computers; many have external ports to enable remote maintenance by the manufacturer or PBX supplier.
- Hackers are able to enter the PBX system through the port used by the manufacturer or PBX supplier by using or breaking passwords.
- Once hackers have access to the PBX they can make calls through the PBX system incurring call charges.

Note: PBX systems that are linked to the Internet are easier for hackers to target; therefore increased security of passwords for these systems is essential.

How does Concert help you fight telephone fraud?

As a Concert customer, we take a number of measures to help you limit the damage a hacker can do via your PBX systems. All your numbers with us are monitored 365 days a year for the following:

- Specific known fraudulent destinations
- Specific known fraudulent numbers
- Short calls
- Long calls
- Locked calls and high cost calls

Concert's Hosted Telephony Solution is however the ultimate protection against fraud. With a centrally hosted and managed telephone solution, customers cannot be exposed to the risk of people hacking into their system, giving complete peace of mind.

For more information on Concert's Hosted Telephony Solution please call us on 0808 208 2400 or [click here to download our Hosted Telephony datasheet](#).

PBX fraud - how to minimise the risk

Unfortunately there is no way to guarantee against fraud. However the simple steps below can make it much harder for hackers to gain access to PBX systems. The following checklist will help you minimise the risk of telephone fraud:

Password management

- ✓ All organisations should have a written policy for password management.
- ✓ Passwords should be changed on regular basis, i.e. at least monthly.
- ✓ Passwords should be a complex combination: a mix of letters, numbers capitals and symbols.
- ✓ There should be a policy in place to change passwords as staff change roles or leave the company, especially those with access to PBX systems.

Contract terms

- ✓ Ensure you have confirmed with your PBX maintainer who is contractually responsible for PBX security/access. If the PBX is accessed via the internet check firewalls are up to date.

Call barring

- ✓ The PBX should be set to bar outgoing calls to premium rate international numbers.
- ✓ Extensions should be limited to required call types (e.g. does the telephone in the post room need access to mobile phones?).
- ✓ Set up CPS call barring (e.g. do you need premium rate international numbers?).

If you suspect fraud

- ✓ Emergency outbound call suspension can be implemented by calling Concert's dedicated support team on **0808 208 2400**.

For more information on how to reduce the risk of telephone fraud please contact us on 0808 208 2400.