

Combating Telephone Fraud with 8el's CallPort

Modern phone systems offer increased levels of functionality that are primarily designed to increase the efficiency of the legitimate users of that system.

However, as with many useful tools, they can be exploited by certain elements of society to further their own aims without regard to the rightful owner. Recently, there have been a number of instances of fraud carried out using telephone systems that end up costing the owners in the form of huge and unexpected bills.

There are a number of types of this fraud, all relying on being able to access voicemail and forwarding services remotely. This is of course a very useful feature for today's mobile workforce, but the very usefulness of this has made the committing of the fraud easier.

For example, if a fraudster can access the forwarding services of an extension, they can simply forward the call to an international or premium rate number and the bulk of the cost (or all of it if the extension has a direct Freephone number) will be charged to the owner of the phone system.

8el's CallPort offers the advanced functionality that could be vulnerable to this type of fraud, so there are some sensible precautions that should be taken in the first instance. There are also some features of CallPort that help to minimise the risk.

Sensible Precautions

Good password policy – Not just for telephony, any device or system that uses passwords would benefit from this.

The fraudsters have knowledge of default passwords for different systems and are very good at guessing a lot of the easy to remember passwords that users set.

A good password policy within an organisation is vital, and users should be encouraged to choose strong passwords (mix up letters and numbers, don't use common words, not too short) and change them regularly.

A little inconvenience for users in the short term could save a lot of pain and cost in the longer term.

Regular checking of setups - If a fraudster does manage to gain access, it will normally be done when it is least likely to be quickly detected, so regular checking is a good idea, especially after weekends.

CallPort Strengths

Firstly, CallPort does not support Direct Inward System Access (DISA), a system that allows users to access telephony features remotely.

Whilst CallPort has the ability to incorporate remote users into an organisation's system via public Internet, this access is controlled by the Session Border Controllers, which are very secure media firewalls.

Even if someone managed to get past them, they would still need to know logins, passwords, hot-desk codes and PINs in order to be able to make calls through the system.

CallPort's voicemail system is not able to access outside lines, so simply accessing a mailbox via a telephone will not give anything more than access to that user's voicemails. Be aware that this may give a competitor or interested party access to sensitive information, so it is well worth making sure that numeric voicemail passwords are also securely managed.

CallPort's forwarding facilities are accessed via a web portal rather than through voice access, which is unusual in itself and therefore less likely to be targeted unless the fraudsters have prior knowledge of the system. This is the area where good password policy is of primary importance.

8e/ are also able to pro-actively monitor call costs and quickly alert customers if any call exceeds a cost threshold. This is normally used to detect employee fraud within the organisation, but would also warn of possible external fraud at an early stage.

Although 8e/ are proud of the fact that no CallPort customer has been successfully defrauded during the two and a half years that it has been on the market, we continue to keep security high on the development agenda.