Data Sheet

GUIDE TO TELECOMS FRAUD

There are several types of telecoms fraud and many names – phone hacking, dial-through fraud, phreaking and PBX fraud. All result in a business paying for calls it did not make.

Telecoms fraud generally involves a third party making long duration calls at the expense of a business. Hackers gain access to a telephone system and generate profit from the calls they make to international premium rate numbers.

Some of these frauds are perpetrated by disgruntled employees, but most are the result of criminals hacking into your network.

Here is a brief overview of how fraudsters access telephone systems:

Direct inward system access (DISA)
This feature allows a caller to dial into the telephone system, enter an authorisation code and get an outbound line. A hacker can then use this feature to make calls at the company's expense.

Voicemail system
Many voicemail systems are equipped with an outbound divert feature with calls directed to a preset number whenever new voicemail messages are received. If a hacker gains access to the voicemail system password and changes the preset number to a premium number, the system will automatically call these and the company will be charged.

Automated attendant
An automated attendant answers the line and invites the caller to enter the extension of the person they called. The caller can then enter a code which gets them an outside line if they know, or can work out, the password.

How to help protect your business
We advise using a number of practical steps to minimise the risk of fraud including:

- Frequently change passwords (including voicemail), especially when employees leave
- Ensure passwords are random - do not use the default ones
- Have unwanted features disabled where possible
- Implement an effective call barring plan
- Check your network provider can alert you quickly when an excessive charge is incurred
- Ensure your telephone system is fully up to date and has current software/security levels
- Conduct a security audit of your telephone system like you would any of your IT systems
- Ensure your staff are fully trained on your telephone system so they fully understand how to use its features and the risks involved

If you need assistance with any of these recommendations, please call 01392 268244.

Fraud Management Service
swcomms monitors your call activity on a daily basis to look for call profiles that do not fit your normal business traffic. When we detect such activity we take action to contact you and alert you to the situation.

We also limit customers' liability to £750 per CLI for any instance of fraudulent activity when customers take our Fraud Management Service.

If we are unable to contact you, because the fraud is happening over a weekend for example, we can put measures in place to cease the calls.

South West Communications Group
Communications House, Moor Lane,
Sowton, Exeter EX2 7JF
T: 01392 369369 www.**swcomms**.co.uk