Crownhill Associates

smart electronic solutions

Don't Use SMS for Confidential Communication

A mobile phone operator dismissed two workers for providing copies of a user's Short Message Service (SMS) messages to a third party. A prime example of why sensitive information should not be transferred via plain text using SMS.

On 19 November 2002, Philip Nourse, a university student in England, was sentenced to five months in prison for obtaining personal data, performing unauthorized modification of a computer program and harassment.

Nourse obtained copies of his girlfriends SMS messages, not from her mobile 'phone, but from employees of mm02 the mobile network operator.

In the case of Nourse the motivation was rather petty, but never the less, it shows how easily SMS data can be obtained for criminal or other nefarious use. Nourse, accessed his 19- year-old girlfriends account on the Friends Reunited web altered her details and pasted photographs of the two having sex. Nourse also printed up explicit pictures of her which he planned to post around the area in which she lived and accessed her email account to direct her friends to explicit images of her posted online.

Nourse obtained proof of his girlfriend's infidelity by persuading two employees at mmO2, to intercept her text messages and pass them on to him.

A spokeswoman for mmO2 advised that this security breach was possible because of a breach of trust by two engineering workers. mm02 dismissed the workers and they have subsequently been convicted for offences under the Data Protection Act in July 2002. Each worker received a fine.

All SMS messages can be viewed by the network operator's systems and personnel. SMS in itself is NOT a technology that can be considered secure.

In this case the breach of security was internal and relied on compromising the integrity of persons in privileged positions. Could a similar breach of security allow a third party to monitor SMS or other private communications by directly accessing the operators network systems, without proper authorisation?

Current telecommunications standards not only accept that monitoring will take place, but specifically provide methods and procedures for the interception of user traffic. These methods and procedures are designed to give Governments and law enforcement agencies legal access to information.

If such systems are in place for legal interception of user traffic, a breach of security by an operator employee could lead to these very powerful tools falling into the hands of the criminal community.

Further, see: Interception References.

Conclusion: we have reservations about the security of GSM communications and in particular SMS text messaging. We are concerned about the safety of personnel who rely on the integrity of SMS text messaging. Further, consideration should be undertaken in relation to SMS text voting in local elections.

Standard SMS text messaging should not be used for any confidential communication.