

Don't Use SMS for Confidential Communication

Nick Jones

A mobile phone operator dismissed two workers for providing copies of a user's Short Message Service (SMS) messages to a friend. The case shows why enterprises should not send private messages via SMS.

NEWS ANALYSIS

Event

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. Among other activities, he posted highly personal information to his ex-girlfriend's Web space on the "Friends Reunited" site, and persuaded two friends at the mobile phone operator mmO2 to send him copies of her SMS communications. mmO2 dismissed the two employees.

Analysis

This event highlights two important points for anyone using consumer technologies such as SMS for business purposes:

- SMS is not a secure environment.
- Breaching security often occurs more easily by concentrating on people rather than technology.

The contents of SMS messages are known to the network operator's systems and personnel. Therefore, SMS is not an appropriate technology for secure communications. Most users do not realize how easy it may be to intercept. Also, in this case, it would likely have been relatively complex to hack into mmO2's systems from an external source to obtain the content of SMS messages. But finding staff privileged to look at the SMS messages and persuading them to reveal the contents proved easier.

This incident illustrates the reservations Gartner has already expressed about security in U.K. trials of SMS voting in local elections held in May 2002. We advise European enterprises, including governments, to issue immediate guidelines that staff should not use SMS for any confidential communication. Enterprises seeking secure communication channels to mobile employees should consider encrypted e-mail channels such as those provided by virtual private networks or devices, such as the BlackBerry by Research in Motion, which have additional security features. To minimize the likelihood of future interceptions, mobile operators should also review their procedures that allow staff access to the texts of SMS message.

Analytical Source: Nick Jones, Gartner Research

Recommended Reading and Related Research

- "SMS Voting Is a First Step Toward Mobile Democracy" — Mobile technology will enable new forms of political behavior, but present technologies raise concerns about usability and security. **By Nick Jones**
- "Mobile and Wireless Security: Worst and Best Practices" — Mobile devices with wireless data and Internet capabilities are leading a new personal computing revolution, and enterprises should develop ways of minimizing security risks. **By John Girard**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509