

16 November 2007

By: Bogdan Popa, Security and Search Engines Editor



[Users Send Embarrassing Emails to the Wrong Person](#)

According to new research

Nowadays, the email is a vital component in a company because it assures the communication between the firm and its connections from all over the world. But the email is not always a secure way to communicate on the web as a recently conducted survey revealed that most companies are afraid that their internal data might be leaked through email. The research conducted by Sophos included 200 respondents, 70 percent of them answering yes when asked if they are "worried about sensitive data leaking from their company via email." 30 percent of the respondents said no according to a press release published by the company. Security vendor Sophos conducted one more survey, questioning the employees if they "ever accidentally sent an embarrassing or sensitive email to the wrong person from work." The numbers were shocking as 50 percent of the employees said they already sent embarrassing messages to another person. In this context, the data leakage is pretty dangerous because some messages that reach another inbox might contain private information about the employees or about the company which obviously can be accessed by the person who receives it. "As more and more business, and indeed personal interaction, is conducted via work email, the risk of slipping up and clicking send without double-checking the recipient's details is ever-growing," said Graham Cluley, senior technology consultant at Sophos. "The fact that as many as half of employees have experienced that heart-stopping moment when they realise that their message is hurtling towards the wrong person shows that the human error factor is too significant to ignore. Businesses would be wise to check that their email security solutions have the facility to prevent this from happening by identifying when sensitive data or attachments are contained in the message, and if they don't, to consider a more water-tight alternative."