



## Putting the 'S' back in security

Internet shoppers are becoming more security savvy, according to a new poll conducted by web usability consultancy Webcredible1.

The poll, which questioned internet users on what makes them trust a website, found that 40 per cent of respondents look for the S after http in the URL before committing to an online purchase.

Https indicates that the Internet connection is secure and information such as credit card details will be encrypted. However, the poll also reveals that a number of internet users are putting their trust in the wrong place.

For example, 28 per cent of respondents stated that dealing with the website of a reputable brand provided the most reassurance when buying online, while 16 per cent confirmed that they judge a website's security primarily on its professional look and feel.

"It's surprising, but very encouraging, to see that so many online shoppers understand the importance of essential security measures like https," says Trenton Moss, director of Webcredible. "However, it's frightening to see that some internet users will naively put their

trust in a website based solely on the way that it looks."

- Research commissioned by NetBenefit reveals that one in three mid-sized companies do not have a disaster recovery plan in place for their website, risking online revenue streams and brand reputation.

Of the 67 per cent of companies that do have plans in place to guard against threats, only 38 per cent test their plans more than once a year.

The research also highlights that many mid-sized companies are underestimating the effect of downtime with 64 per cent of respondents anticipating no damage or only slight damage if their website goes down for a day.

- NTA's Web Application Security Report 2007 shows that 90 per cent of UK organisations' websites contain one or more vulnerabilities that may enable external users to gain unauthorised system access or disrupt service availability. A further 33 per cent of websites contain critical vulnerabilities which are widely known and exploited by hackers.