

November 11, 2010

Security risk of online shopping at work

Graham Snowdon

[Share](#) · [print](#) · [T+](#) [T+](#) · [T-](#)



AP Employees browse on office computers. Shopping online using office computers puts employers at an increased risk of virus and phishing attacks. File photo

Employees who use work computers to shop online for Christmas presents are putting their employers at increased risk of viral internet threats such as malware and phishing attacks, according to a report.

While the annual survey into workers' internet seasonal shopping habits, conducted by the U.K. Information Systems Audit and Control Association (ISACA), suggests employees will spend far fewer work hours shopping online this year - an average of six hours compared with 14 last year - it says the risk of them clicking on dubious or unauthenticated email links, or divulging personal information to unverified websites, is greater.

This is mainly due to more employees using company mobile devices such as notebook computers, tablets or smart phones, which increase a company's security risk when used on wireless networks outside of protected corporate networks, the report said. They are also more easily lost or stolen, and contain corporate data that is typically not encrypted.

The increased use of social networks for purchasing goods is also cited as an added risk.

Mark Lobel, a mobile security project leader with ISACA and adviser at PricewaterhouseCoopers, said: “The number of portable computers and mobile devices in the workplace is only going to increase, so companies need to create a realistic security policy that lets employees stay mobile without compromising intellectual property.” But security was not a major concern for participants in the survey, with around two-thirds saying they do not use secure browsing technology on work-supplied devices. Around half the workers surveyed assumed their IT department kept them up to date on security patches.

ISACA has issued a series of tips for workers using company computers or devices for online shopping:

- Do not click on an email or web link from an unfamiliar sender or looks “too good to be true”.
- Be careful with company information that can be accessed through your mobile device (it suggests using a privacy screen shield).
- Password-protect your mobile device and its memory card.
- Make sure the security tools and processes protecting your work-supplied mobile devices are kept up to date.

Copyright: Guardian News & Media 2010