Who started it? Makes no matter.
Tip of the month from Internal Audit

Feb 25, 2009

This is part of a continuing series of monthly tips from Ohio University’s Office of Internal Audit that address common errors, misunderstandings and control failures often found during audits. Internal Audit performs departmental and process reviews, working collaboratively with units to assess and improve controls across the university.

Even if you understand that sensitive data should not be sent via e-mail, be aware that a reply or forward of an e-mail may allow sensitive data to continue on a dangerous path.

It is not unusual to reply to an e-mail, including the original text, only to realize later that the e-mail contained sensitive data.

Follow these basic requirements for good and secure handling of sensitive data.

- Do not request or send social security or credit card numbers via e-mail.
- Do not reply to or forward an e-mail that contains such numbers.
- Do not send attachments that include such information, even if the attachment is password-protected.

There may be other ways to expose sensitive data as well. If you are handling or need to share sensitive data, please contact the Ohio University Information Security Office at 740-566-SAFE for guidelines and advice.

-- From staff reports