

Fake Amazon Order Emails

Trading Standards Officers are urging computer users to be wary of spoof emails purporting to be from online retailer Amazon.

The emails purport to be order confirmations for high value items such as televisions, and claim that the said items have been shipped to the recipient's address. They carry a .zip file attachment which opens what appears to be a Word document. However, the said file is in fact malware that will compromise the security of the user's PC.

Officers advise recipients to delete such emails immediately and not to open attachments under any circumstances.

Effective online security is crucial, and users should ensure that their PCs are running up-to-date anti-virus, anti-spyware and firewall software. Internet Explorer 6 users should upgrade their browsers without delay, and all users should ensure that their operating systems are kept fully patched by installing published security updates promptly.

Crucially, Internet security software should be supported by user commonsense and awareness of Internet-based threats. For this reason, Officers advise PC users to read up on online security via www.getsafeonline.org. They also advise turning off any 'auto-preview' features in their email software, and encourage all email users to follow their advice for avoiding email spam ([Avoiding Spam](#)).

Produced: 17th May 2010

All our alerts are available in a range of formats and languages, including large print. Please contact Community Development if this would be helpful to you, or to someone you know. Address: 14 Martin Street, Stafford, ST16 2LG

