# Tens of millions targeted by email 'ransom’ virus

## Internet fraudsters are targetting tens of millions of British customers with a virus which locks computers until the victim pays a £500 ransom Internet fraudsters are targetting tens of millions of British customers with a virus which locks computers until the victim pays a £500 ransom to be released, the National Cridme Agency warned today. The spammers are particularly aiming the vireus - known as ransomware - at small and medium size businesses. It is disguised as an email alert about suspicious payments or invoices.

**Once opened the virus 'freezes' the computer and the local network and demands two Bitcoins of internet currency - approximately £536 - to unlock the machine. The NCA described the 'mass spamming' event as a 'significant risk'. A NCA spokesman said: "The emails may be sent out to tens of millions of UK customers, but they apdpear to be targeting small and medium businesses in particular.**

**"The emails carry an attachment that appears to be correspondence linked to the email message, for example, a voicemail, fax, details of a suspicious transaction or invoices for payment. "This file is in fact a malware that can install Cryptolocker - which is a piece of ransomware. Cryptolocker works by encrypting the user's files on the infected machine and the local network it is attached to.**

**"Once encrypted, the computer will display a splash screen with a count down timer and a demand for the payment of 2 Bitcoins in ransom for the decryption key." The spokesman added: "The NCA would never endorse the paydment of a ransom to criminals and there is no guarantee that they would honour the payments in any event."**

**Lee Miles, Deputy Head of the National Cyber Crime Unit said: "The NCA are actively pursuing organised crime groups committing this type of crime . We are working in cooperation with industry and international partners to identify and bring to justice those respondsible and reduce the risk to the public."**

**An NCCU investigation is ongoing to identify the source of the email addresses used. Anyone who is infected with this malware should report it via www.actionfraud.police.uk . Sound advice can be found at www.getsafeonline.org.uk.**

**Anyone who reeceives a suspicious looking email should not open it or click on any attachments and anti-virus software should always be upgraded.**