

29 August 2008

By: Denisa Ilascu, Internet / SEO News Editor



Hitman email scam continues to trick people artbeyond

## [The FBI: "Do Not Open Unsolicited E-mails"](#)™

### *The Bureau warns about hitman email scams*

The FBI has decided to take more measures to fend off the wave of spam attacks in which the sender pretends to be a hitman hired to kill the recipient of the email, or a loved one. The Internet Crime Complaint Center (IC3), a branch of the federal authority, has released an official note, advising people not to listen to the demands of a supposedly paid criminal who claims thousands or even tens of thousands of dollars (depending on their eagerness to become rich) from the victim.

"Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. Providing your PII [personally identifiable information] will compromise your identity!" says the IC3 advisory.

Although these attempts to extort money from people were first reported back in 2006, July 2008 was the month when the attacks began to proliferate. Security organizations have made it clear that all that targeted people need to do is to delete the malicious emails and go on with their lives (which had not been threatened for a second, in fact).

However, regardless of this, some still fall for the trick. In order to persuade the victims that the threat is as real as it gets, scammers also include some of the victims' personal details, which can usually be found on personal blogs, social network profiles or official documents posted on the Internet.

It seems like the instinct of self-preservation can actually be blinding for many, as they can no longer tell the difference between a valid threat and a scam. Whenever someone receives a messages revealing the terrible secret that one of their friends went and hired a hitman to get them killed, they should rest assured that, at least in 99% of the cases, it's nothing more than an extortion attempt. Also, those who have received (or will in the future) such malicious emails are advised to [report](#) it to the appropriate governmental institutions.