

Als er einmal auf die cipav.exe klickte

FBI-CIPAV.exe Is an
Unknown Application.
Install Anyway?

[Heise](#) über das FBI, das einen [Artikel fälschte](#), um Malware auf dem Rechner eines Verdächtigen [zu installieren](#):

Dafür fälschten sie einen angeblich von der Nachrichtenagentur AP stammenden Artikel über Bombendrohungen und verschickten einen Link darauf an einen [MySpace-Account](#). Als der Verdächtige darauf klickte, sei ihm die Software „Computer and Internet Protocol Address Verifier“ (CIPAV) auf dem Rechner installiert worden“.

Merke: Der Verdächtige hatte Windows (sonst hätte es nicht funktioniert). Der Verdächtige las unverschlüsselte E.Mails. Der Verdächtige las unverschlüsselte E-Mails von fremden Personen. Der Verdächtige klickte auf Links in E-Mails (er verhielt sich grob fahrlässig, weil er HTML-E-Mails empfing und sie auch so anzeigen ließ). Der Verdächtige war grob unvorsichtig und hatte Javascript *nicht* verboten (nur so ginge das). Der Verdächtige surfte vermutlich über einen Admin-Account und wurde nicht beim Installieren einer Software gefragt. Der Verdächtige verhielt sich denkbar bescheuert.

Übrigens stammt die Geschichte aus der [Wired](#) aus dem Jahr 2007: „The software was sent to the owner of an anonymous MySpace profile linked to bomb threats against Timberline High School near Seattle. The code led the FBI to 15-year-old Josh Glazebrook, a student at the school, who on Monday pleaded

guilty to making bomb threats, identity theft and felony harassment."