

# Drive-by hacking on the rise

[Technology](#), [Development](#)



Web-drive-by attacks--sounds like some New York gangster movie? Maybe, but attacking web users where they feel most safe for example at home on their computer, at work protected by corporate network security, can cause as much harm as getting robbed on the street.

*Trend Micro* : " Web-drive-by attacks may not harm you physically but they definitely could harm your wallet, steal precious personal data or even take over your whole computer system".

Visiting certain websites may be as dangerous as the risk of having your belongings stolen by taking a short cut down a dark alley way at night. Until recently, both consumer and corporate IT users knew to be careful before clicking on certain unsolicited e-mails which may contain computer viruses. But as malware threats change and evolve, users are increasingly being affected by simply visiting a website. Web threats are increasingly being identified as the next type of threat to be aware of. Some websites contain potentially dangerous downloaders which install themselves on your PC without you noticing. Once installed, these can monitor and steal your passwords as well as bombard you with targeted spam. This has implications particularly for corporate users browsing a large number of websites on a day-to-day basis, sometimes as part of their job.

A report on e-crime recently published by the London Police, which deals with the majority of e-crime in the UK pointed out that e-crime is the most rapidly expanding form of criminality, encompassing both new criminal offences in relation to computers (viruses and hacking) and 'old' crimes (fraud and harassment) committed using digital or computer technology. The

cost of identity theft to the UK economy alone is estimated at 1.7bn [pounds sterling] a year. A panel of leading experts discussed the future of the internet at the World Economic Forum in Davos. Vint Cerf, one of the fathers of the internet expressed his worry on cyber crime at the event stating that he believed up to a quarter of computers on the net may already be used by cyber criminals in so-called botnets. Trend Micro warns that enterprises need to take a careful look at their policy reinforcement with regards to web surfing. CIOs should educate users and ask them to be more vigilant in their web browsing behaviour. But how do you know which websites are safe, and which to avoid?