

Che cos'è uno Spy-Ware?

DEFINIZIONE

Uno **spyware** è un tipo di [software](#) che raccoglie [informazioni](#) riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite [Internet](#) ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di [pubblicità](#) mirata

COME SI DIFFONDONO

Uno spyware può essere installato sul [computer](#) di un ignaro utente semplicemente visitando delle [pagine Web](#), scaricando programmi gratuiti da internet. In alcuni casi, la stessa applicazione che promette di liberare dagli spyware ha in realtà installato spyware o è essa stessa uno spyware

PRINCIPALI RISCHI E DANNI CAUSATI DAGLI SPYWARE

Gli spyware costituiscono innanzi tutto una minaccia per la [privacy](#) dell'utente, in quanto carpiscono senza autorizzazione informazioni sul suo comportamento quando connesso ad Internet: tempo medio di navigazione, orari di connessione, siti Web visitati, se non dati più riservati come gli indirizzi [e-mail](#) e le [password](#). Le informazioni raccolte vengono inviate ad un computer remoto che provvede ad inviare pubblicità mirata sulle preferenze ricavate dall'analisi del comportamento di navigazione. Gli annunci possono essere ricevuti sotto forma di [pop-up](#), [banner](#) nei siti Web visitati o nel programma contenente lo spyware o, nei casi più invasivi, [posta elettronica](#) non richiesta ([spam](#)). Talvolta lo spyware è utilizzato da vere e proprie organizzazioni criminali, il cui obiettivo è utilizzare le informazioni raccolte per furti di denaro tramite i dati di [home banking](#) o tramite i numeri di [carta di credito](#)

COME DIFENDERSI DAGLI SPYWARE

L'arma migliore per difendersi dagli spyware è diffidare da qualsiasi software offerto gratuitamente su Internet: come detto l'inclusione in programmi molto scaricati è il mezzo più frequente di diffusione di questi malware. Evitare di visitare siti "sospetti", come quelli che offrono [software pirata](#) o [crack](#) è un'altra precauzione salutare, così come l'astenersi dal seguire i link contenuti nei messaggi di [spam](#) (posta indesiderata) ricevuti nella casella di posta elettronica.

La presenza di un [antivirus](#) può non essere sufficiente a proteggere dagli spyware, dato che essi non sono virus o worm, **si rende quindi necessario utilizzare software appositamente concepiti a difendersi da questa minaccia.**

Informazioni tratte da Wikipedia.