PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 24 di martedì 11 gennaio 2000

Privacy on line: la crittografia alla portata di tutti

Presentato il sistema 'Freedom' che consente di proteggere le comunicazioni via Internet. L'altro lato della medaglia: il sistema potrebbe favorire azioni illegali.

Le informazioni fornite durante le comunicazioni effettuate via Internet lasciano tracce che permettono la ricostruzione e l'analisi di alcuni dati riguardanti l'utente.

Per garantire la privacy del navigatore la societa' canadese Zero Knowledge propone un programma che consente sia di proteggere con la crittografia le comunicazioni via Internet (e-mail, chat, acquisti, newsgroup), sia di mantenere l'anonimato fornendo all'utente pseudonimi detti 'Nym'.
Il costo del programma e' di circa 100.000 lire.

Il sistema si basa su una catena di server: i dati in partenza dal computer vengono 'imbustati' in involucri crittografati, ogni server della catena apre un involucro e legge l'indirizzo del server successivo. I server della catena sono in grado di conoscere solo 2 indirizzi, quelli dei server contigui.

Alcuni obiezioni sono state sollevate riguardo alla liceità di questo tipo di strumenti, in quanto se da un lato il sistema parrebbe proteggere la privacy dell'utente, dall'altro potrebbe favorire operazioni illegali.

---

www.puntosicuro.it