

## COS'È UN KILL SWITCH? TUTTO QUELLO CHE C'È DA SAPERE SU DI ESSO NEL 2022

23 Agosto 2022



Nel senso più generale della parola, un kill switch si riferisce a un meccanismo che fa sì che una macchina si spenga improvvisamente quando qualcosa va storto. Può anche essere usato per descrivere un simile arresto di emergenza nel software invece che in un macchinario fisico.

Un kill switch per il software

Come per le macchine, anche alcuni software fanno uso di un kill switch. Pensate, per esempio, al software usato dalle

grandi aziende che raccolgono molti dati degli utenti, o al software governativo che contiene ogni sorta di informazioni sensibili. Se il software finisce nelle mani di persone non autorizzate, un kill switch può assicurarsi che non vedranno nessuno di questi dati sensibili. Senza la giusta autorizzazione, la persona che cerca di accedere alle informazioni non le otterrà. I dati saranno resi invisibili o inaccessibili. Il kill switch potrebbe anche cancellare completamente il software. In questo modo, qualsiasi informazione sensibile rimane fuori dalle mani sbagliate.

Perché le VPN hanno un kill switch?

La maggior parte delle persone che [usano migliore VPN](#), lo fanno per proteggere la loro privacy. Desiderano rimanere anonimi mentre navigano in internet, e una VPN può aiutare in questo. Se la tua VPN dovesse temporaneamente non funzionare, tuttavia, rimarresti senza protezione. I tuoi dati saranno inviati su internet senza la protezione aggiunta di un tunnel VPN. Di conseguenza, il tuo indirizzo IP sarà comunque visibile al mondo esterno. È qui che entra in gioco il kill switch.

Un kill switch VPN assicura che non andrai mai online senza protezione. Se la tua VPN non funziona correttamente mentre stai navigando, il kill switch spegnerà del tutto la tua connessione a Internet. Per tutto il tempo in cui la VPN soffre di problemi di connessione, non sarai in grado di navigare, fare streaming o scaricare nulla. Dal momento che la tua intera connessione a Internet viene interrotta, il tuo vero indirizzo IP rimarrà protetto e la tua privacy rimarrà intatta. Gli hacker non saranno in grado di arrivare ai vostri dati. In altre parole, il kill switch assicura che la VPN ti protegga, anche quando non funziona come dovrebbe.

Perché la mia connessione VPN dovrebbe cadere?

Una connessione VPN che cade può avere molteplici cause. Ecco alcune delle più frequenti:

Cattiva connessione internet: Se stai lavorando con una connessione internet instabile per cominciare, è probabile che la tua VPN possa vacillare. Questo potrebbe essere il caso quando stai usando una rete Wi-Fi con un segnale debole, per esempio. Passare costantemente da una rete all'altra ha un effetto simile.

Problemi con il server VPN: Un'altra possibile causa è il server VPN stesso. Se un server sta sperimentando un qualche tipo di malfunzionamento interno, questo può far cadere la tua connessione VPN nella sua interezza. I problemi potrebbero essere causati dalla forza del segnale del server, da interruzioni nel server fisico o da semplici time out della connessione. Inoltre, quando un particolare server viene utilizzato da molte persone allo stesso tempo, diventa sovraffollato. In questi momenti, spesso si verificano anche dei problemi: la connessione può diventare incredibilmente lenta o cadere del tutto.

Impostazioni di firewall, antivirus o router: Un altro possibile fattore ostacolante potrebbe nascondersi nelle impostazioni di altri programmi sul tuo dispositivo. Alcuni programmi hanno impostazioni specifiche che, se attivate, non permettono alla tua VPN di stabilire una connessione. Un firewall o un programma antivirus potrebbero vedere la connessione esterna [della VPN](#) come un rischio. Di conseguenza, cercheranno di bloccare la VPN, trasformando il tuo tunnel sicuro in una connessione irregolare e inaffidabile. Anche il tuo router e gli aggiornamenti automatici del tuo dispositivo potrebbero causare problemi di questo tipo.

Quali VPN hanno un buon kill switch?

In generale, le persone considerano un kill switch un'aggiunta positiva a qualsiasi servizio VPN. Per la sua stessa natura, un kill switch attivato potrebbe impedirti di andare online per un certo periodo di tempo. Tuttavia, nella maggior parte dei casi, questo batte l'alternativa: essere senza protezione su internet. Il kill switch aumenta la tua privacy online e ti aiuta a mantenere il controllo della tua connessione internet.

Molte VPN hanno un kill switch. Alcuni provider richiedono di attivarlo a mano cambiando le impostazioni, mentre altri provider lo hanno attivato di default. Tuttavia, alcuni provider VPN sono migliori di altri. Quelli che hanno una funzione kill switch e possono essere raccomandati sono [ExpressVPN](#), CyberGhost e NordVPN.