La Redazione

Più sicurezza, Alexa!

Fatti e misfatti della smart home

Secondo un'analisi sul mercato digitale, il numero di abitazioni con dispositivi di smart home attivi dovrebbe raggiungere i 573,7 milioni di utenti entro il 2026, con una diffusione prevista pari al 25%. Ma un recente rapporto di Kaspersky commissionato ad Arlington Research su 21.645 proprietari di dispositivi smart home in 21 Paesi, tra cui Stati l'Italia, mostra che alla discreta conoscenza dei prodotti per la smart home e delle loro funzionalità non corrisponde altrettanta attenzione per la sicurezza. E questo nonostante le paure di essere hackerati siano presenti in gran parte degli utenti.

Più della metà degli intervistati teme infatti che la propria rete domestica o il router Wi-Fi vengano violati o hanno paura di essere spiati attraverso il sistema di telecamere connesso a Internet (56%). L'integrità dei sistemi di monitoraggio domestico o dei dispositivi di sicurezza connessi al Wi-Fi o a Internet che spiano gli utenti è un problema per il 53% degli intervistati. E non si tratta invero di falsi problemi, dal momento che i data breach registrati nei dispositivi intelligenti coinvolgono pressoché tutti i prodotti (tende avvolgibili, sistemi di schermatura Wi-Fi, apparecchiature mediche come monitor della pressione sanguigna ma anche sistemi di irrigazione intelligenti). Il 12% delle violazioni riguarda porte, serrature e campanelli intelligenti.

Nel 2026 le case dotate di dispositivi di smart home saranno 573,7 milioni, il 25% della popolazione

Come ci si protegge

Tuttavia le vaste campagne di sicurezza cyber messe in campo pare stiano raggiungendo anche i proprietari di dispositivi intelligenti, che mostrano mediamente di avere discrete abitudini digitali: il 51% sceglie infatti di utilizzare una soluzione di sicurezza informatica; il 41% cambia regolarmente la password e aggiorna il software del dispositivo e il 34% acquista solo da produttori affidabili (ritenendo la fiducia nel brand un elemento sufficiente per avere una protezione adeguata).

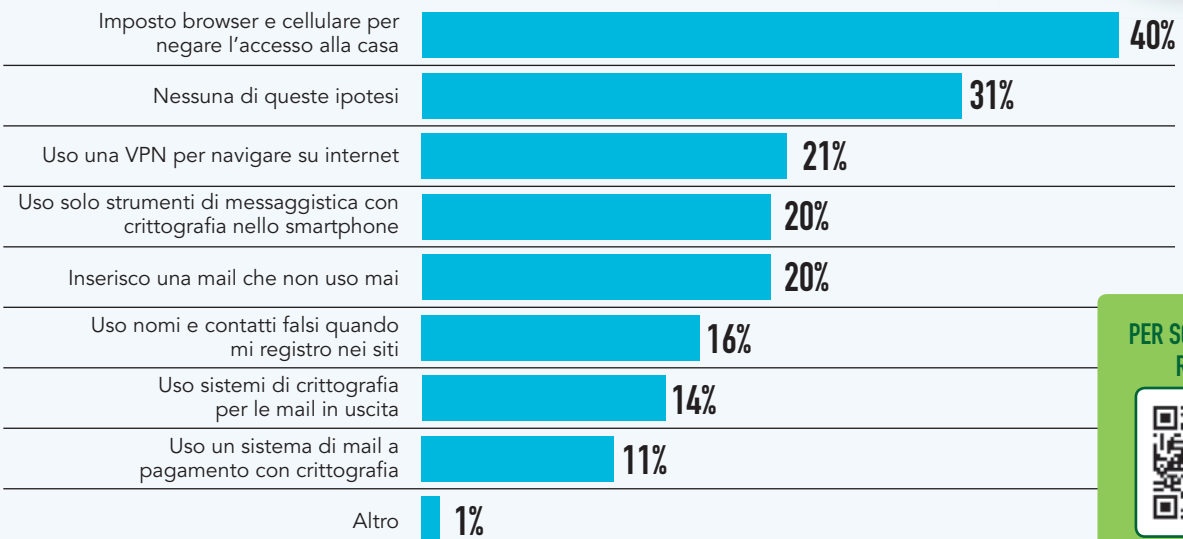
L'esperto consiglia

Per proteggere tutti gli smart device, gli esperti di Kaspersky consigliano di:

- non acquistare dispositivi smart home di seconda mano (il firmware potrebbe essere stato modificato dai precedenti proprietari per permettere ai cyber criminali di controllare gli ecosistemi smart home)
- cambiare la password predefinita con una password complessa e aggiornarla regolarmente
- proteggere la rete mantenendo riservati i numeri di serie, gli indirizzi IP e altre informazioni sensibili. Non condividere i dispositivi smart degli utenti sui social network
- installare una soluzione di sicurezza cyber affidabile per proteggere l'intero ecosistema della smart home (e ricordare che comprare un gadget "che gestisce l'allarme o gli accessi" non significa installare un vero sistema di sicurezza! ndR)
- essere sempre aggiornati sugli ultimi update e sulla scoperta di vulnerabilità dopo aver scelto un'applicazione o un dispositivo particolare. Installare tempestivamente tutti gli aggiornamenti rilasciati dagli sviluppatori.

Un prodotto per smart home che controlla l'allarme e gli accessi non può quasi mai essere considerato un vero sistema di sicurezza

Come si protegge chi usa dispositivi per la smart home?



Fonte: The smart home of almost everything, una ricerca Kaspersky

PER SCARICARE IL REPORT