## Come proteggere casa da un attacco hacker: robot aspirapolvere, frigo, smart tv, videocamere di sicurezza e router di Saverio Alloggio

**Gli apparecchi connessi possono essere violati, usati per spiare o arruolati nelle botnet. Che cosa rischia ogni dispositivo, perché quelli a basso costo sono i più esposti e come difendersi**
**(Fonte: https://www.corriere.it/ 14 novembre 2026)**



Gli attacchi che tra ottobre e novembre hanno mandato in tilt i banchi frigo di centinaia di supermercati europei, Italia compresa, hanno riportato l'attenzione su un rischio che riguarda anche le case. «Gli apparecchi domestici sono spesso trascurati sul fronte della sicurezza, ricevono aggiornamenti di rado, e una falla presente in migliaia di modelli identici può essere sfruttata su larga scala», spiega Marco Fanuli, Technical Director di TrendAI Italia, business unit di Trend Micro. «Con una famiglia il calcolo è un altro: una singola casa ha poco valore, quindi i criminali puntano sulla quantità più che sul singolo bersaglio».

Indice


- Che cos'è una botnet
- Dispositivo per dispositivo: i robot aspirapolvere
- Frigoriferi, forni e lavatrici
- Smart TV e TV box
- Videocamere di sicurezza e baby monitor
- Router: come proteggere la rete wi-fi domestica
- Serrature, allarmi e videocitofoni

- Assistenti vocali, prese e lampadine
- Il rischio dei marchi sconosciuti e a basso costo
- Che cosa prevede il Cyber Resilience Act
- Le password e le altre regole per tutti i dispositivi

**Che cos'è una botnet**

Quella quantità ha un nome: **botnet**. È una rete di apparecchi infettati, a volte centinaia di migliaia, che obbediscono a un unico centro di comando senza che i proprietari se ne accorgano. Ogni dispositivo continua a fare il suo lavoro, ma nel frattempo esegue gli ordini dei criminali: inondare di traffico un sito fino a renderlo irraggiungibile, inviare spam, provare password rubate su migliaia di account, oppure fare da ponte per chi commette truffe online, che così appare collegato da una normale casa italiana.

Il caso di scuola è Mirai, che nel 2016 riunì centinaia di migliaia di telecamere e videoregistratori violati con le password di fabbrica e rese irraggiungibili per ore servizi come Twitter e Netflix. I suoi eredi sono ancora più grandi. Nel 2025 la botnet **Aisuru**, composta soprattutto da router e apparecchi domestici compromessi, ha battuto più volte il record mondiale di attacco per volume di traffico, superando i 30 terabit al secondo. A giugno dello stesso anno l'FBI ha lanciato l'allarme su **BadBox 2.0**, oltre un milione di dispositivi infetti, quasi tutti TV box, proiettori e tablet economici senza marchio. Per il proprietario le conseguenze sono invisibili ma concrete: connessione più lenta, indirizzo di casa segnalato come sospetto dai servizi online e un intruso stabilmente dentro la rete domestica.

**Dispositivo per dispositivo: i robot aspirapolvere**

I modelli più evoluti hanno telecamera, microfono e una mappa dettagliata della casa, salvata quasi sempre sui server del produttore. Nell'ottobre 2024, negli Stati Uniti, alcuni robot sono stati violati e usati per insultare i proprietari dall'altoparlante e inseguire gli animali domestici. Nel febbraio 2026 un programmatore che voleva soltanto guidare il proprio robot con il controller di una console si è ritrovato, per una falla nei server del produttore, a poter comandare circa 7 mila apparecchi in 24 Paesi.

**Le difese sono semplici**. Se la telecamera serve solo a evitare gli ostacoli, la visione da remoto va disattivata nell'app, così come il microfono quando non si usano i comandi vocali. **L'account va protetto con una password unica e la verifica in due passaggi,** e il **firmware** va aggiornato appena disponibile. Prima di vendere o regalare il robot, va eliminato dall'account per cancellare le mappe della casa.

**Frigoriferi, forni e lavatrici**

I **grandi elettrodomestici connessi** custodiscono pochi dati sensibili, ma sono computer a tutti gli effetti, aggiornati di rado, e un apparecchio vulnerabile diventa una porta d'ingresso nella rete di

casa. A fine settembre, in Corea del Sud, un aggiornamento distribuito per errore da Samsung ha bloccato a distanza alcuni frigoriferi: nessun criminale, ma la prova che un elettrodomestico collegato può essere fermato da lontano. I frigoriferi con schermo e fotocamere interne, poi, sono veri tablet in cucina, con browser e account collegati, e vanno trattati come tali.
**La prima domanda da porsi è se la connessione serva davvero**: un frigorifero o una lavatrice offline continuano a funzionare come prima. Se le funzioni smart si usano, l'apparecchio va collegato alla rete separata descritta più avanti e tenuto aggiornato. Molti forni chiedono di abilitare il controllo a distanza dal pannello prima di accettare comandi dallo smartphone: conviene farlo solo quando serve. Nella stessa famiglia rientrano condizionatori, caldaie e termostati connessi, con un rischio in più: un intruso potrebbe alterare temperature e consumi.

**Smart TV e TV box**
Sono tra i bersagli preferiti delle **botnet**. BadBox ha colpito soprattutto TV box economici che promettono migliaia di canali gratis, spesso venduti con il software malevolo già installato o infettati da app scaricate fuori dagli store ufficiali. Le smart TV dei marchi noti sono più protette, ma raccolgono molti dati: diverse registrano ciò che passa sullo schermo per profilare la pubblicità. Il televisore va aggiornato e le app vanno installate solo dallo store ufficiale. Nelle impostazioni sulla privacy si possono disattivare il riconoscimento dei contenuti visti e la pubblicità personalizzata.
Telecamera e microfono, presenti in alcuni modelli o nel telecomando, **vanno disattivati se non servono**. Un televisore che non riceve più aggiornamenti può essere scollegato da Internet e usato con un box o una chiavetta di un marchio noto. **Un TV box senza marchio e senza aggiornamenti, invece, è meglio lasciarlo sullo scaffale**.

**Videocamere di sicurezza e baby monitor**
Sono i dispositivi più delicati, perché riprendono gli interni e spesso hanno un microfono: un accesso abusivo significa qualcuno che guarda e ascolta. A volte basta un errore del produttore. Nel febbraio 2024 un marchio statunitense di videocamere economiche, dopo un guasto ai server, ha mostrato per sbaglio a circa 13 mila clienti le immagini delle case di altri utenti.



La password di fabbrica va cambiata al primo avvio e l'account protetto con la verifica in due passaggi. Meglio scegliere modelli con otturatore fisico o modalità privacy, registrazione in locale su scheda di memoria e, se si usa il cloud, **crittografia end-to-end**. Le telecamere interne si possono spegnere quando si è in casa e vanno posizionate in modo da non inquadrare camere da letto e bagni. Per vedere le immagini da fuori casa va usata l'app ufficiale, senza aprire porte sul router. Negli impianti più vecchi il punto debole è spesso il videoregistratore a cui sono collegate le telecamere: va aggiornato e protetto con la stessa cura del router. Per i neonati, un baby monitor a radiofrequenza che non si collega a Internet elimina il problema alla radice.

**Router: come proteggere la rete wi-fi domestica**

Il router è la porta d'ingresso di tutta la casa connessa: se viene compromesso, diventano raggiungibili tutti gli apparecchi e la navigazione può essere dirottata verso siti fasulli. Aisuru è cresciuta proprio sui router poco protetti.

Il pannello di gestione si apre dal browser con l'indirizzo riportato sull'etichetta. Vanno cambiate la **password di amministrazione**, diversa da quella del wi-fi, e quella della rete, di almeno dodici caratteri, con cifratura WPA3 o WPA2 con protocollo AES. Vanno disattivati il WPS, l'UPnP, che permette agli apparecchi di aprire varchi verso Internet senza chiedere il permesso, e la gestione remota del pannello. La misura più efficace è collegare robot, elettrodomestici, telecamere e prese a una rete separata, come quella per gli ospiti: se uno viene violato, l'intruso non raggiunge computer e smartphone. Dopo lo spostamento va verificato che tutto funzioni, perché alcuni apparecchi devono dialogare con l'hub sulla rete principale, e una volta al mese conviene

controllare l'elenco dei dispositivi collegati ed eliminare quelli sconosciuti. Un modem dell'operatore molto vecchio, che non riceve più aggiornamenti, va fatto sostituire.

**Serrature, allarmi e videocitofoni**

Controllano l'accesso fisico alla casa, e per questo meritano la massima attenzione. **Conviene preferire marchi con una politica di aggiornamento dichiarata**, attivare le notifiche per ogni apertura, proteggere l'account con la verifica in due passaggi e mantenere sempre un'alternativa meccanica, come una chiave o un codice di emergenza. Se l'apertura da remoto non serve, le serrature che funzionano via Bluetooth o con un codice possono restare scollegate da Internet.

**Assistenti vocali, prese e lampadine**

Gli **smart speaker** ascoltano in attesa della parola di attivazione: il tasto fisico che spegne il microfono va usato nelle conversazioni riservate, e dall'app si può rivedere e cancellare la cronologia delle registrazioni. Se l'assistente comanda serrature o allarmi, l'apertura a voce va protetta con un PIN. Prese e lampadine intelligenti sono i dispositivi più economici e più spesso senza marchio: proprio per questo vanno confinate sulla rete separata. Prima di comprarle conviene verificare che funzionino con l'ecosistema già presente in casa, così da gestire tutto con un'unica app affidabile invece che con tante app diverse.

**Il rischio dei marchi sconosciuti e a basso costo**

Sui **marketplace** si trovano telecamere a 15 euro, TV box a 25 e prese a pochi euro l'una. Dietro molti di questi prodotti c'è lo stesso schema: un unico fabbricante produce l'apparecchio e lo cede a decine di rivenditori, che lo vendono con nomi diversi, spesso sigle di poche lettere, e con la stessa app generica. Una falla in quel software colpisce così, nello stesso momento, centinaia di migliaia di dispositivi di marche apparentemente diverse. Password uguali per tutti e talvolta impossibili da cambiare, aggiornamenti rari o assenti, server gestiti da società difficili da identificare, app che chiedono accesso a contatti e posizione senza motivo: i problemi si ripetono. Nei casi peggiori, come per BadBox, il software malevolo è installato in fabbrica. E quando il marchio sparisce dal mercato, l'app smette di funzionare o resta senza correzioni.
Anche marchi noti hanno avuto falle gravi: conta chi corregge i difetti e per quanto tempo. I segnali d'allarme sono un nome senza sito ufficiale, l'assenza di manuale e assistenza in italiano, nessuna indicazione sulla durata degli aggiornamenti, una dichiarazione di conformità europea introvabile, recensioni che lamentano un'app abbandonata.

**Che cosa prevede il Cyber Resilience Act**

Il **regolamento europeo 2024/2847** sulla sicurezza dei prodotti connessi obbliga dall'11 settembre 2026 i fabbricanti a segnalare entro 24 ore le vulnerabilità sfruttate e ad avvisare gli utenti coinvolti, anche per i prodotti già in commercio. In Italia la vigilanza è affidata all'Agenzia per la

cybersicurezza nazionale. Dall'11 dicembre 2027 ogni nuovo apparecchio venduto nell'Unione, ovunque sia fabbricato, dovrà avere una configurazione sicura di fabbrica e almeno cinque anni di aggiornamenti gratuiti, con la data di fine del supporto indicata al momento dell'acquisto. Per telecamere, serrature, baby monitor e router i controlli saranno più severi, con sanzioni fino a 15 milioni di euro o al 2,5% del fatturato mondiale. Gli apparecchi già installati nelle case, però, restano fuori dai nuovi requisiti.

**Le password e le altre regole per tutti i dispositivi**

Ogni account va protetto con una **password diversa e lunga**, gestita con un password manager, ormai integrato in telefoni e browser. Il riutilizzo è l'errore più pericoloso: le credenziali rubate a un sito vengono provate in automatico su migliaia di altri. La verifica in due passaggi, che aggiunge alla password un codice temporaneo generato da un'app o inviato via sms, va attivata prima di tutto sull'app che governa la casa connessa e sull'email. Lo smartphone che fa da telecomando va tenuto aggiornato e protetto con un blocco schermo.

Prima di comprare conviene cercare sul sito del produttore la data minima fino alla quale sono garantiti gli aggiornamenti e preferire dispositivi compatibili con lo **standard Matter**, che funzionano nella rete di casa senza passare per forza dai server del produttore. Quando il supporto finisce, l'apparecchio va isolato o sostituito, e prima di venderlo va rimosso dall'account e riportato alle impostazioni di fabbrica. Un dispositivo che si muove, parla o si accende da solo, una spia della telecamera accesa senza motivo, accessi all'account da luoghi sconosciuti sono segnali da non ignorare: bisogna scollegarlo, cambiare la password, chiudere le sessioni attive e ripristinarlo. In caso di accessi abusivi, immagini diffuse online o ricatti, la denuncia va presentata alla Polizia Postale, anche attraverso il Commissariato di P.S. online.