I DISPOSITIVI IOT NELLE NOSTRE CASE

Nelle nostre case sono ormai presenti molti dispositivi che per **funzionare richiedono una connessione a Internet**: smartphone, TV, computer, pannelli solari, telecamere di sicurezza e molti altri. Questi strumenti rendono la vita più comoda, ma se non sono correttamente gestiti possono diventare una porta d'ingresso per gli attaccanti.

I RISCHI DERIVANTI DAI DISPOSITIVI IOT

I rischi derivanti dai dispositivi IoT che impattano sulla nostra vita quotidiana possono essere distinti come segue:

PERDITE ECONOMICHE

I criminali impersonificano banche, corrieri, etc. tramite e-mail o messaggi fraudolenti nel tentativo di convincere la vittima a condividere le sue credenziali, con evidenti danni economici.

RISCHIO PRIVACY

Telecamere di sorveglianza o assistenti vocali potrebbero essere compromessi dai criminali per registrare o trasmettere contenuti delle nostre vite private.

RISCHIO PER L'IDENTITÀ DIGITALE

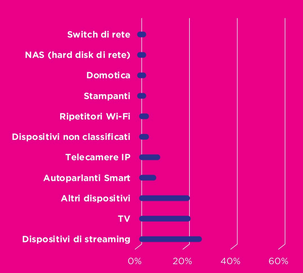
Una password debole o riutilizzata può permettere agli attaccanti di assumere il controllo degli account e causare danni reputazionali ed economici.

RALLENTAMENTI E MALFUNZIONAMENTI

I dispositivi IoT possono essere violati dai criminali e successivamente utilizzati per i loro attacchi, rallentandone il funzionamento o interrompendolo.

I DISPOSITIVI IOT PIÙ ESPOSTI ALLE MINACCE INFORMATICHE

I dispositivi IoT che presentano il maggior numero di vulnerabilità sono i dispositivi di streaming (es. Amazon Fire Stick, Apple TV, etc.) con il 25,94%, seguiti dalle smart TV con il 21,34%.



COME PROTEGGERE I DISPOSITIVI IOT

Per proteggere i nostri dispositivi IoT è necessario adottare misure di sicurezza a livello di rete domestica (router) e di dispositivi connessi.

RETE DOMESTICA

1. **Scegliere una password robusta**. Per la configurazione del router di casa è consigliabile sostituire fin da subito la password impostata dalla fabbrica e scegliere una password complessa, lunga e non facilmente indovinabile (evitando, ad esempio, informazioni personali come la data di nascita o il nome del proprio animale domestico). La password deve inoltre essere unica e non riutilizzata per l'accesso ad altri servizi o account.
2. **Aggiornamenti automatici del router.** Attivare la funzione di aggiornamento del firmware consente di correggere automaticamente eventuali vulnerabilità e mantenere il dispositivo sempre protetto.
3. **Sostituzione del router.** Router datati possono non ricevere più aggiornamenti di sicurezza: è quindi consigliabile sostituirli con modelli più recenti e meglio protetti.

DISPOSITIVI CONNESSI

1. **Autenticazione multifattore (MFA).** Quando disponibile, è consigliabile attivare sempre l'autenticazione a più fattori (ad esempio, tramite codice via SMS o app di autenticazione) per rendere l'accesso ai dispositivi e ai servizi più sicuro.
2. **Aggiornamenti di sicurezza.** Installare tempestivamente gli aggiornamenti consente di correggere vulnerabilità e proteggere i dispositivi da possibili attacchi.
3. **E-mail e messaggi sospetti.** In caso di richieste urgenti di condivisione di dati (es. credenziali di accesso all'home banking) o di pagamenti, anche se provenienti da mittenti noti, è importante verificare sempre l'autenticità del mittente prima di agire, ad esempio, contattandolo tramite un canale diverso da quello su cui è arrivata la comunicazione, poiché potrebbe trattarsi di una truffa.

Fonte: The 2025 IoT security landscape report di Bitdefender