

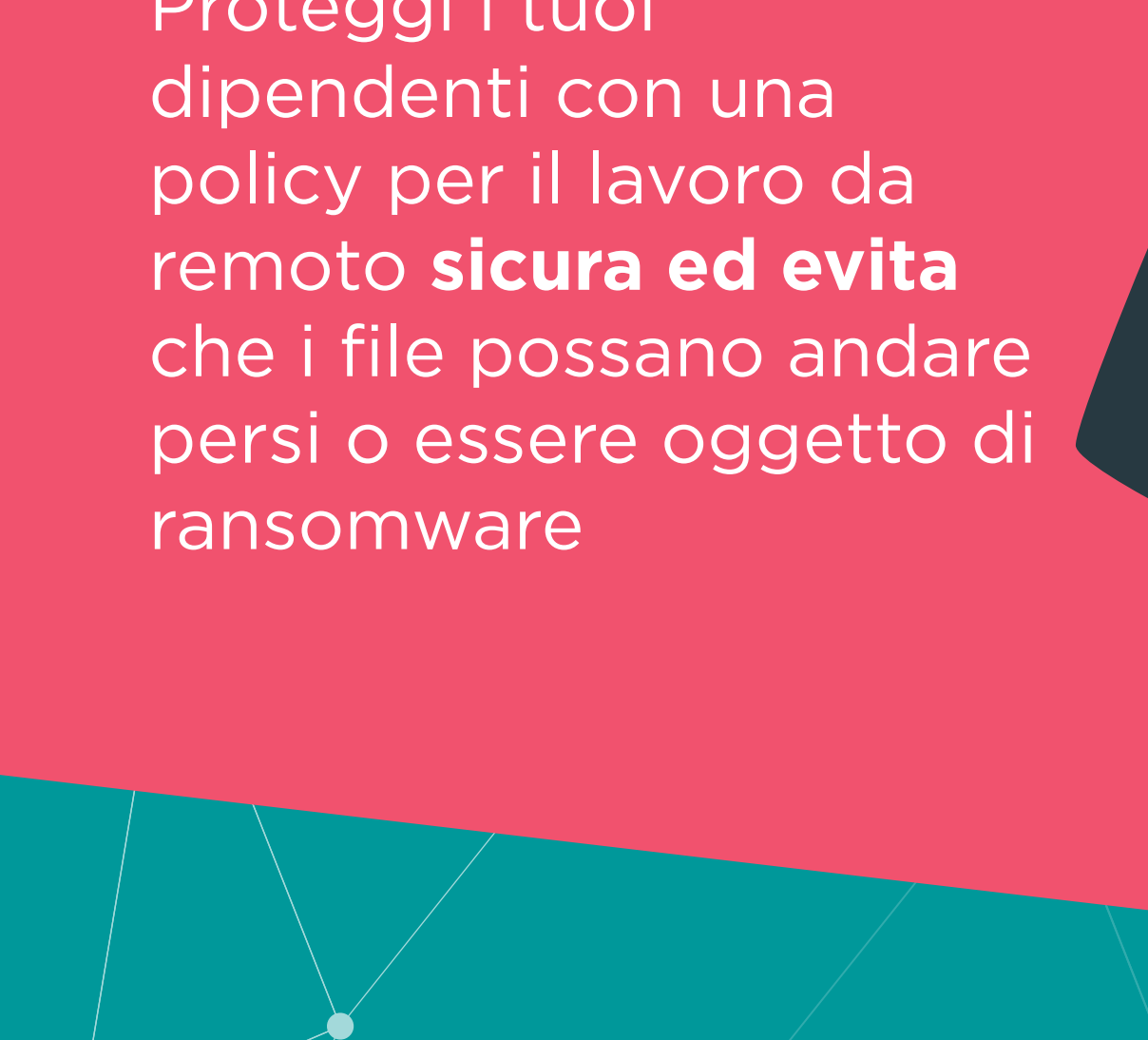
GARANTIRE LA SICUREZZA DEL LAVORO DA REMOTO

Un terzo dei decision-maker IT ammette che le loro aziende hanno subito una violazione dei dati a causa del lavoro da remoto¹. Alla luce di ciò, come è possibile garantire che i dati dell'azienda rimangano protetti durante questi periodi di emergenza?

01.

Metti in sicurezza il lavoro da remoto della tua azienda

Una rete per ufficio domestico ha **3,5 volte più probabilità** di essere infettata da malware rispetto a una rete aziendale²



Gli hacker **sanno** se dietro il PC c'è un utente domestico o un utente aziendale che lavora a casa



02.

Diffida degli attacchi di phishing

Le e-mail di phishing correlate al Covid-19 rappresentano oggi il target principale degli **attacchi**³



Le truffe sono aumentate di oltre il **400%** nel solo Regno Unito nei mesi di febbraio e marzo⁴, con una perdita complessiva di oltre 1,6 milioni di sterline per le vittime⁵

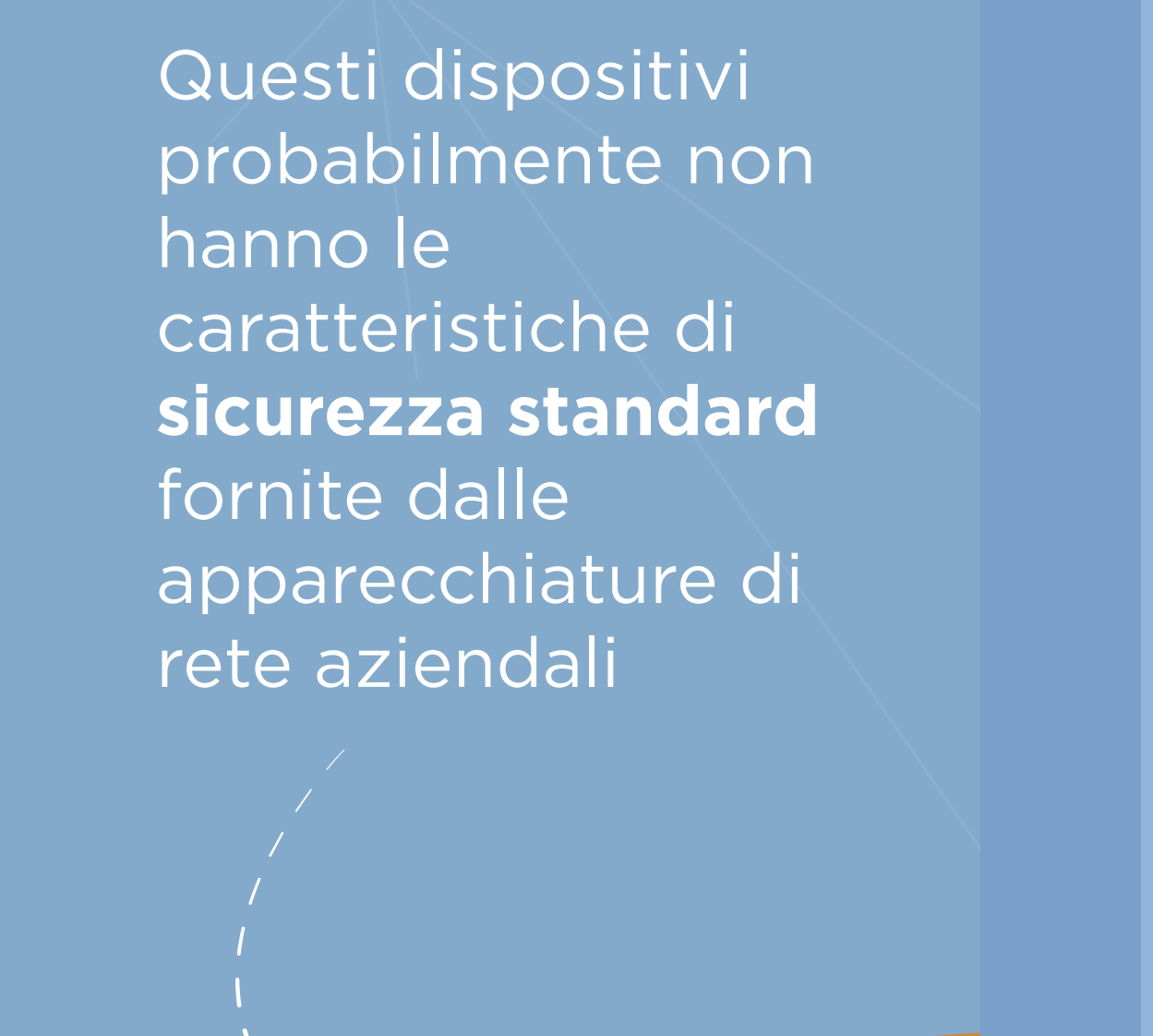


Assicurati che i tuoi dipendenti **controllino il mittente di un'e-mail prima di aprirla**. Inoltre, anche prima di fare clic su link sconosciuti, dovrebbero fare tutte le verifiche del caso



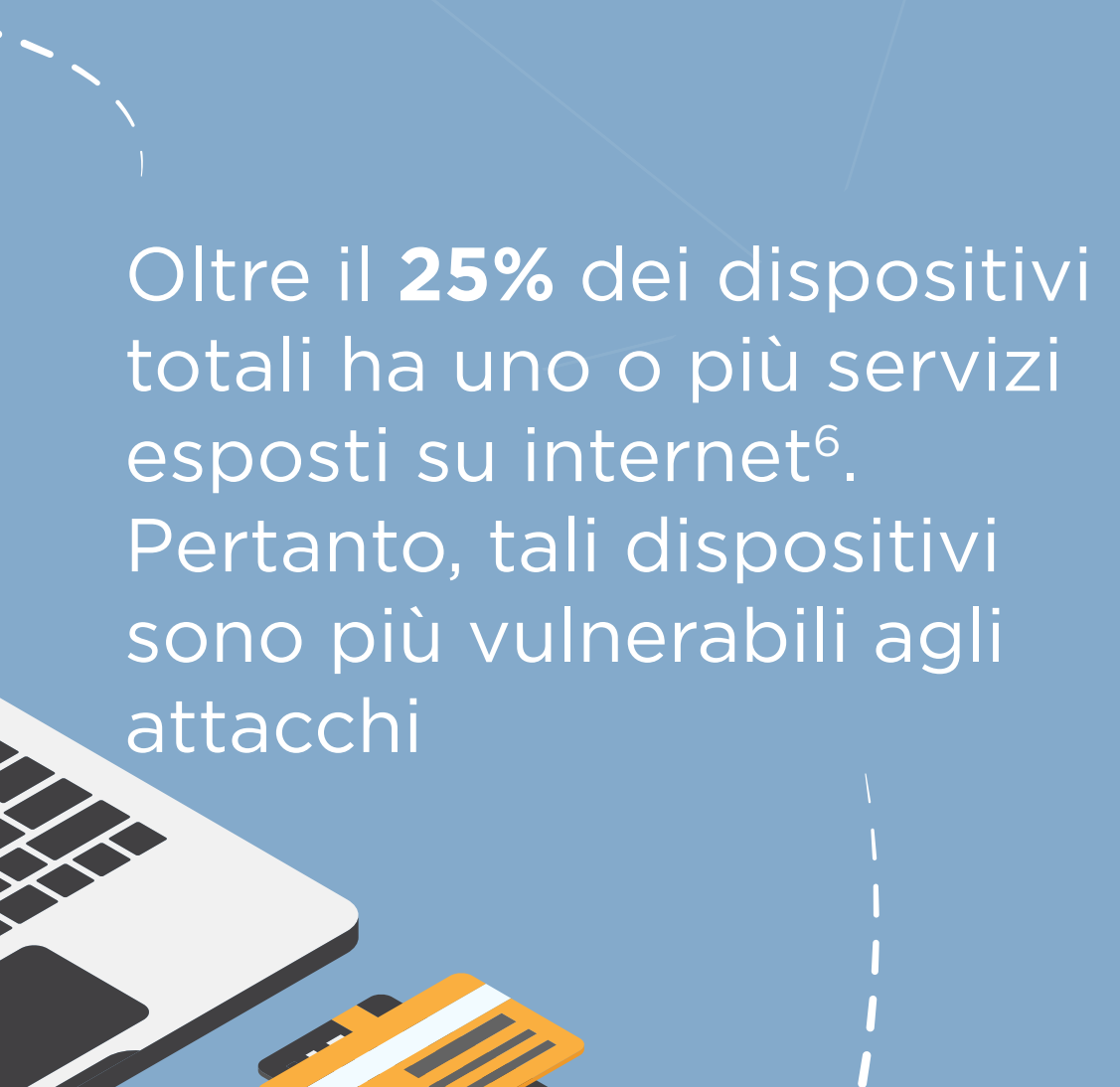
03.

Non dimenticare la sicurezza dei dispositivi di casa



Lo staff utilizzerà sicuramente le stampanti e gli scanner disponibili a casa

Questi dispositivi probabilmente non hanno le caratteristiche di **sicurezza standard** fornite dalle apparecchiature di rete aziendali



Oltre il **25%** dei dispositivi totali ha uno o più servizi esposti su internet⁶. Pertanto, tali dispositivi sono più vulnerabili agli attacchi



Per salvaguardare i tuoi dati aziendali sensibili, fornisci ai tuoi dipendenti il supporto necessario per garantire che la loro rete sia privata e che vi si possa accedere solo con una password **sicura** e non predefinita



04.

E i documenti riservati

Assicurati che chi lavora da remoto tratti i documenti aziendali con la stessa cura con cui tratta i suoi estratti conto bancari, assicurandosi di distruggere o conservare in modo **sicuro qualsiasi documento** riservato fino a quando non sarà possibile tornare in ufficio



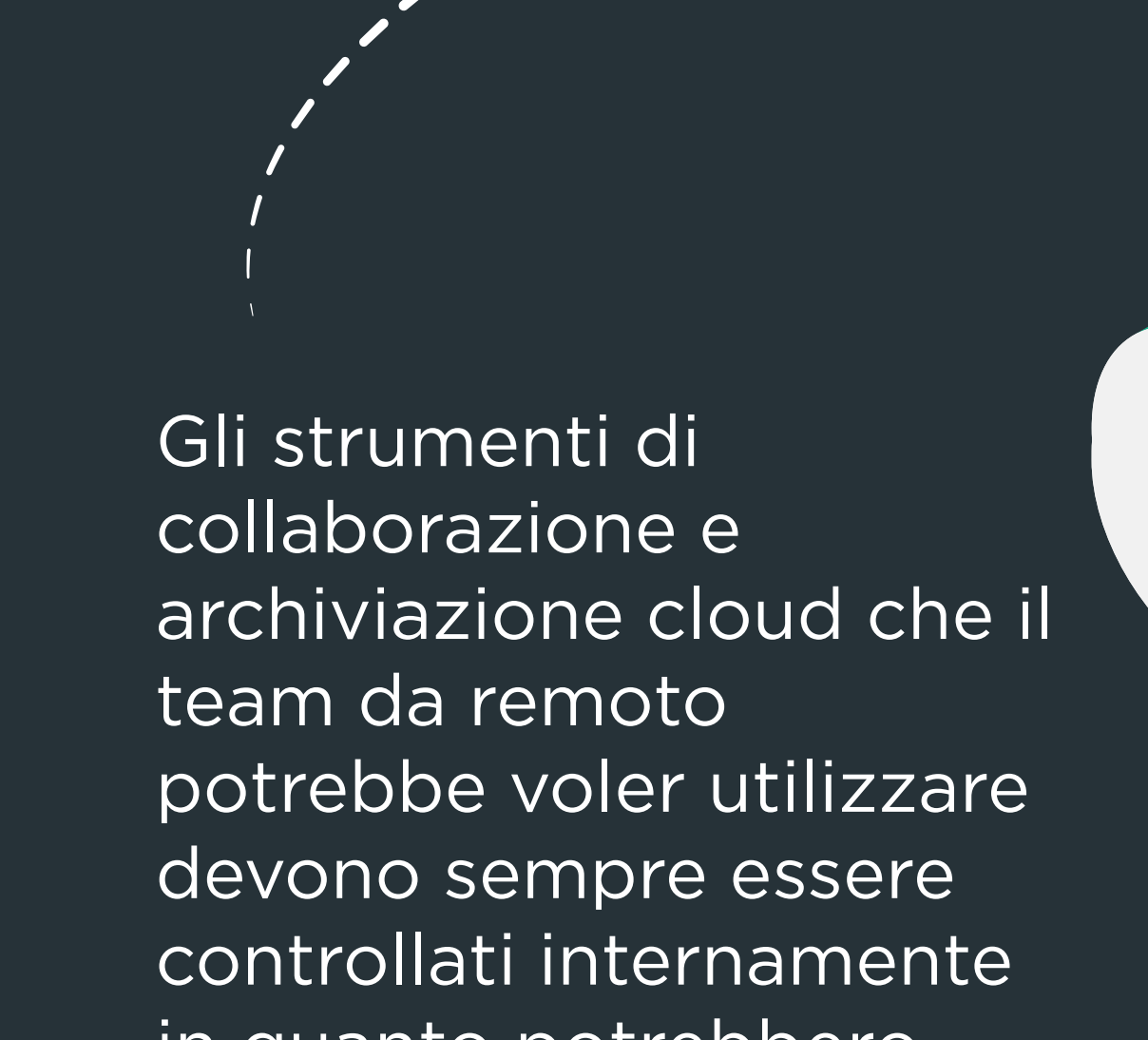
05.

La policy migliore è...averne una

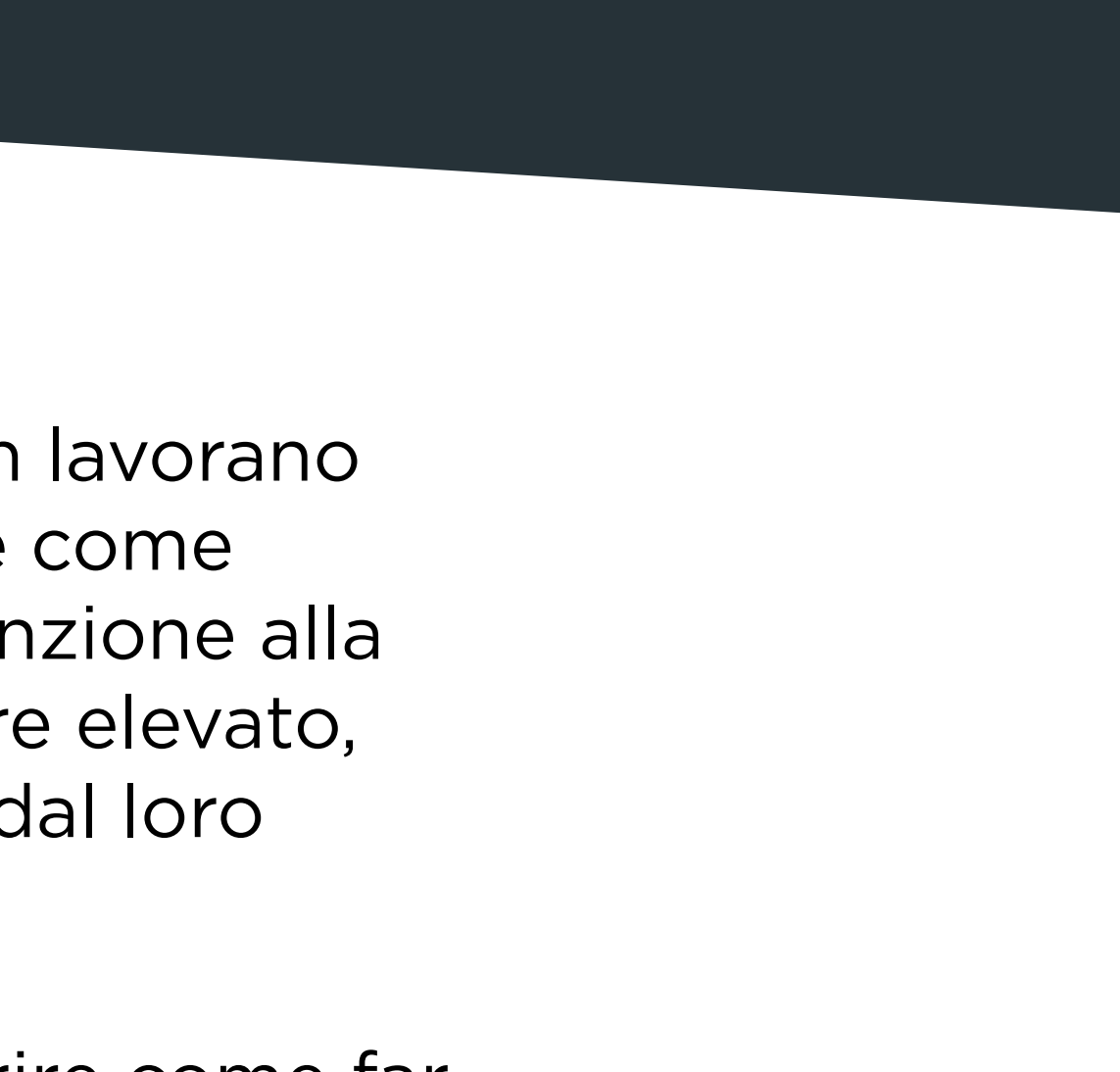
Smart working **non vuol** dire perdere il controllo sulle attività dell'azienda



Ricorda al team di utilizzare solo le applicazioni, le reti e il **cloud aziendali**



Gli strumenti di collaborazione e archiviazione cloud che il team da remoto potrebbe voler utilizzare devono sempre essere controllati internamente in quanto potrebbero **non essere sicuri**



Se alcuni membri del team lavorano da remoto, devono sapere come mantenere il livello di attenzione alla sicurezza aziendale sempre elevato, che lavorino dall'ufficio o dal loro salotto.

Contatta Canon per scoprire come far crescere l'azienda in questo periodo di incertezza, anziché limitarti a farla sopravvivere.

Canon

See the bigger picture

¹ <https://www.zdnet.com/news/cybersecurity/covid-19-cybersecurity/>

² <https://www.zdnet.com/news/cybersecurity/covid-19-cybersecurity/cybersecurity/covid-19-cybersecurity/>

³ <https://www.bbc.com/news/technology-54423541>

⁴ <https://www.actiontrust.police.uk/alerts/coronavirus-related-fraud-reports-increase-by-400-in-march>

⁵ <https://www.thebusinessdesk.com/news/standards/news/20200301-the-perils-of-remote-working-the-next-normal-in-data-protection>

⁶ <https://www.bright.com/blog/identifying-unique-risks-of-attacks-from-home-remote-office-networks>