

10

consigli per rendere lo Smart Working sicuro ed efficiente



LAVORA IN VPN

Ogni utente deve avere un account con diritti limitati, i dati devono essere criptati e le connessioni tra home worker, sedi periferiche e sede centrale devono avvenire con tunnel VPN. Evita collegamenti con un Desktop Remoto non cifrato, ma utilizza VPN sicure SSL/IPSEC.



VEICOLA IL TRAFFICO TRAMITE VPN

Veicola la navigazione Internet in modo che passi attraverso un firewall hardware che, se opportunamente configurato e con le necessarie appliance di sicurezza, può fornire una prima linea di difesa.



CONFIGURA UN FIREWALL DOMESTICO

Implementa un firewall VPN per garantire la permanenza in una connessione point-to-point protetta e privata e comunicazioni aziendali VPN affidabili e sicure. I servizi Anti-Virus e Web Filter sono altamente consigliati per garantire protezione da minacce informatiche.



UTILIZZA UN COMPUTER AZIENDALE

L'utilizzo di un pc personale può causare problemi alla rete perchè non dispone dei livelli di protezione di un device aziendale.



UTILIZZA LA CONNETTIVITÀ MOBILE A BANDA LARGA

Grazie a un router mobile Wi-Fi indoor/outdoor, navighi velocemente, liberamente e in sicurezza da casa. Sfrutta la rete mobile per i tuoi collegamenti!



NO A SITI WEB NON SICURI

Non visitare siti web non sicuri, in particolar modo blog e piattaforme che potenzialmente contengono più minacce (es. presenza di numerosi pop-up, adv, ecc...).



ATTENZIONE ALLE MAIL

Fai attenzione anche alle email che arrivano da mittenti conosciuti e/o con allegati con estensioni attendibili (.txt, .pdf): anche queste possono contenere virus. Controlla la sintassi, la grammatica e i nomi degli allegati: spesso le email dannose hanno testi errati e di bassa qualità.



AGGIORNA SISTEMI E SOFTWARE

Assicurati che il sistema operativo e le applicazioni siano sempre aggiornati. È consigliabile utilizzare le ultime versioni disponibili.



PASSWORD COMPLESSE

È importante usare password complesse per gli account VPN: evita di usare dati sensibili (date di nascita, nomi, località di residenza) e utilizza caratteri speciali, lettere maiuscole e minuscole.



AUTENTICAZIONE A DUE FATTORI

Per aumentare il livello di sicurezza del tuo account (e quindi della rete aziendale), utilizza l'autenticazione a due fattori con password temporanee.

**E ricorda:
attento alla postura!**



Dota la tua scrivania di monitor, tastiera e mouse. Per il benessere della tua schiena, non lavorare direttamente sul portatile. Allestisci in casa il tuo ufficio!

Vuoi realizzare una VPN sicura?

CONTATTACI

ZYXEL
www.zyxel.it