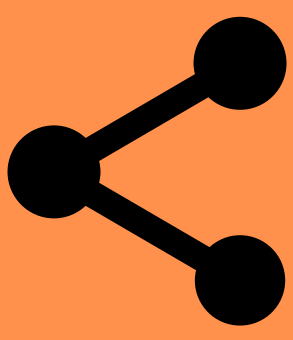
5 Consigli per rendere lo Smart Working sicuro ed efficiente

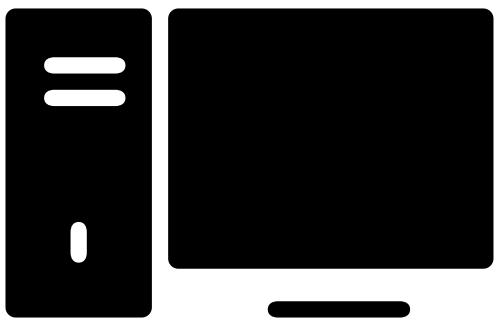


1) LAVORA IN VPN

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 Desktop Remoto non cifrato, ma utilizza VPN sicure SSL/IPSEC.

2) UTILIZZA UN PC AZIENDALE

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

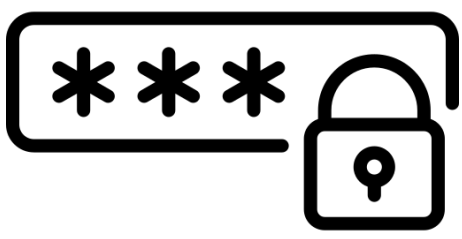


3) CONFIGURA UN FIREWALL DOMESTICO

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 Antivirus e Web Filter sono altamente consigliati per garantire protezione da minacce informatiche.

4) 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 minuscole e maiuscole.



5) AUTENTICAZIONE A DUE FATTORI

Per aumentare il livello di sicurezza del tuo account, utilizza l'autenticazione a due fattori con password temporanee.

E RICORDA ATTENTO ALLA POSTURA!

Per il benessere della tua schiena, non lavorare direttamente dal portatile. Allestisci in casa il tuo ufficio!

VUOI REALIZZARE UNA VPN SICURA?

CONTATTACI

noleggia-facile.it