

Cyber Check List

LE 10 MIGLIORI PRATICHE PER LIMITARE I RISCHI INFORMATICI IN RELAZIONE AL REMOTE WORKING



01

ACCESSO REMOTO

Fornire l'accesso remoto alla rete aziendale attraverso un mezzo sicuro (ad es. VPN).



02

AUTENTICAZIONE

Se possibile, prevedere un doppio fattore di autenticazione.



03

PROTOCOLLI SICURI

Utilizzare i servizi da remoto solo tramite protocolli sicuri (HTTPS).



04

MONITORAGGIO

Porre maggior attenzione ai controlli sui computer collegati in remoto (antivirus, gestione delle patch, ecc.).



05

BLOCCO DA REMOTO

Essere in grado di bloccare i dispositivi da remoto.



06

CRITTOGRAFIA

Assicurarsi che i dispositivi siano crittografati.



07

BACKUP INFORMAZIONI

Effettuare un backup regolare delle informazioni.



08

FORMAZIONE DIPENDENTI

Informare i dipendenti su possibilità di ricezione di phishing, e-mail malevole, ecc.



09

SEGNALAZIONE DELLE MINACCE

Stabilire protocolli specifici affinché gli utenti possano segnalare istantaneamente il verificarsi di qualsiasi situazione anomala o sospetta.



10

CONNESSIONE A RETI SICURE

Evitare o limitare il più possibile la connessione attraverso reti pubbliche e/o non protette.