Il lavoro da REMOTO

10 COSE da ricordare

DPO – ing. E. MALIZIA
www.studiomalizia.it | www.studiomaliziafad.it

1 Ambiente sicuro

E' importantissimo che l'ambiente dove si presta l'attività lavorativa sia il più possibile protetto da interferenze esterne. Anche gli aspetti della vita privata devono essere opportunamente protetti e separati. Utilizzare per quanto possibile profili utente differenziati sui sistemi domestici.

2 Connettività di rete

Diffidare di reti pubbliche o private aperte, senza chiavi di protezione; attraverso le reti wireless non protette possono essere messe in atto diverse tipologie di attacchi da parte di malintenzionati o di malware pericolosi come ramsoware e altri codici malevoli.

3 Sistemi aggiornati

I sistemi informatici, aziendali o privati, devono essere mantenuti costantemente aggiornati per la risoluzione continua di difetti o vulnerabilità di sistema che vengono sempre più sfruttate dalle minacce alla sicurezza alle informazioni.

4 Antivirus aggiornato

Il software antivirus e anti malware deve essere costantemente aggiornato per agire come idonea misura di protezione dalle minacce ai dati e ai dispositivi.
No utilizzare software con licenze scadute o obsoleti, e curare se necessario l'aggiornamento manuale dell'antivirus.

5 Backup

Creare copie dei dati che vengono elaborati sui dispositivi nel lavoro da remoto, se questi non risiedono già nei sistemi informativi aziendali, è essenziale. Utilizzare supporti removibili oppure soluzioni Cloud sicure e crittografate.

6 Software e vulnerabilità

Utilizzare soltanto software idonei, anche sulle postazioni domestiche, aiuta a prevenire da possibili interferenze, cali di prestazioni e altre situazioni di incompatibilità che possono arrecare danni anche importanti alle attività sui sistemi informativi aziendali.

7 Attenzione al phishing

Prestare estrema attenzione alle mail che si ricevono. Le minacce correlate al Social engineering, Phishing, Ramsoware, etc. sono in crescita esponenziale, soprattutto in questa fase di potenziale maggiore vulnerabilità correlata alle attività effettuate con prestazioni da remoto.

8 Crittografia connessioni

Prestare sempre attenzione ai siti web, portali, e VPN che si utilizzano sia per le attività lavorative che per quelle private; diffidare sempre di siti con certificati non affidabili, ad esempio non https, e di canali di trasmissione non sicuri o non affidabili.

9 Password e credenziali

Utilizzare password di complessità sufficiente, anche mediante un software password manager, e ove possibile prediligere l'**autenticazione a più fattori,** sia per l'accesso ai sistemi che per condividere files con colleghi e terzi a cui trasmettiamo informazioni.

10 Logout sicuro

Per l'uscita dalle applicazioni e da servizi web, non chiudere il browser, ma effettuare sempre il logout dai sistemi in modo da chiudere le sessioni applicative. Non salvare le credenziali di accesso ad aree riservate dei siti web nei browser.