CLIENTE	**Innovery**	TESTATA	**Businessinsider.com**	DATA	**16 marzo 2020**

BUSINESS INSIDER ITALIA

#iorestoacasa. 12 regole per lo smartworking in sicurezza (dai cyber attacchi)

In Italia sono circa 570mila i lavoratori che già lavorano da remoto, ma il numero sta crescendo molto rapidamento a causa dell'emergenza Coronavirus. Anche perché le istituzioni spingono in questa direzione con l'obiettivo di limitare al minimo i contatti e dunque la diffusione del virus.

Tuttavia, dietro il lavoro in digitale, esistono rischi che forse non tutti sono pronti ad affrontare, perché lo smartworking resta una novità per molti settori lavorativi, molti dei quali non sono a conoscenza dei pericoli in cui è possibile incorrere. **Innovery Spa,** system integrator specializzato nel comparto cyber security fornisce alcune *best practice* per un'esperienza di telelavoro in sicurezza:

1. Le attività da remoto devono essere svolte unicamente utilizzando le **postazioni di lavoro (notebook in genere) forniti dall'azienda e non avvalersi di PC personali** (neppure per leggere la posta) che generalmente non dispongono di un livello adeguato misure di sicurezza (antivirus, personal firewall, ecc.) in grado di garantire la protezione delle risorse aziendali cui il lavoratore deve accedere per svolgere le proprie mansioni.

2. L'accesso alla postazione di lavoro deve sempre avvenire mediante l'utilizzo di credenziali di autenticazione (login e password) assegnate individualmente dall'azienda al dipendente, le quali **non devono essere condivise** con nessun'altra persona, neppure un componente dello stesso nucleo familiare. Se l'azienda lo consente, utilizzare le funzionalità di autenticazione biometrica messe a disposizione dal sistema operativo adoperato (fingerprint, face recognition).
3. La password di accesso alla propria postazione deve essere conservata in luogo segreto, non deve essere trascritta in post-it attaccati al monitor o conservati nel cassetto della propria scrivania, né comunicata con qualsiasi mezzo ad altra persona. Si suggerisce di **cambiare la password con una frequenza maggiore** rispetto a quanto previsto dalle policy aziendali, poiché potrebbe essere carpita da malintenzionati con maggior probabilità.
4. **Bloccare la postazione di lavoro** (tasto Windows + L) ogni qualvolta ci si allontani da essa; per rafforzare tale misura si suggerisce di configurare un blocco schermo (Screen Saver) con password, che obbliga l'utente a reinserire la password quando sono trascorsi alcuni minuti di inattività (si suggerisce un intervallo non superiore a 10 minuti).
5. La connessione alla rete aziendale deve avvenire mediante una **VPN** (Virtual Private Network), ossia un canale di comunicazione sicuro tra il dispositivo remoto e l'azienda, attraverso il quale si accede direttamente agli applicativi ed ai dati aziendali. Anche la navigazione su Internet deve avvenire sempre tramite la VPN di modo che si possa usufruire delle stesse protezioni di sicurezza (blocco siti pericolosi, proxy, antiphishing, ecc.) che si dispone navigando dall'interno della rete della propria azienda.

6. Attivare la funzione di **cifratura del disco** (mediante le soluzioni consigliate dalla propria azienda) per far sì che, in caso di furto, sia garantita la riservatezza delle informazioni conservate ed eliminando così il rischio di violazioni dei dati personali eventualmente presenti sulla postazione di lavoro.
7. Qualora l'azienda abbia sottoscritto servizi di Private o Public Cloud Storage (ad es. OneDrive, Google Drive, Box.net, ecc.) è opportuno che tutti i dati aziendali presenti sulla propria postazione di lavoro (escludendo i propri dati ad uso personale) vengano memorizzati nelle cartelle locali sincronizzate in real-time con il server in Cloud, al fine di garantire la disponibilità dei dati anche in caso di un guasto del disco. Se non si dispone di tale funzionalità, è necessario effettuare le copie di backup dei dati della postazione di lavoro, con cadenza almeno settimanale, sui supporti di memorizzazione prescelti dall'azienda
8. Tenere sempre aggiornato il sistema operativo all'ultima versione disponibile, abilitando gli aggiornamenti automatici messi a disposizione dal produttore (ad es. Windows Update). **Gli aggiornamenti devono essere installati nel più breve tempo possibile**, al massimo allo spegnimento del PC (selezionando l'opzione Aggiorna ed Arresta).
9. La postazione deve essere dotata del sistema **antivirus** fornito dall'azienda mediante il quale periodicamente avviare la scansione dell'intero disco, al fine di verificare la presenza di malware; tale operazione deve essere svolta con cadenza almeno settimanale oppure essere avviata in automatico quando il PC non è utilizzato.
10. Qualora il lavoratore dovesse accorgersi che la sua postazione di lavoro sia stata infettata da un *malware*, o perché segnalato dall'antivirus o perché si accorge di comportamenti anomali, deve immediatamente scollegarla dalla rete e contattare l'azienda.