S&L
SALUTE E SICUREZZA NEI LUOGHI DI LAVORO

Via G. Bovini 41 – 48123 Ravenna (RA) Tel. 0544 465497 333 1182307
www.sicurezzaoggi.com info@sicurezzaoggi.com

ISO 9001:2015

Prot. 190420/MP

Ravenna, 19 aprile 2020

Oggetto: uso in sicurezza del PC in smart working.

Indichiamo di seguito alcune semplici e utili cose considerare per evitare qualche inconveniente nell'uso del PC.

- Installare **Antivirus** è un software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware per un **computer** come virus, adware, backdoor, BHO, dialer, fraudtool, hijacker, keylogger, LSP, rootkit, spyware, trojan, worm o ransomware. Mantenerlo aggiornato. è una delle cose più importanti che devi compiere per proteggere il tuo PC. È possibile scaricare antivirus gratuiti o a pagamento, questi ultimi offrono spesso qualche funzione aggiuntiva che può tornare sempre utile, come ad esempio di attivare delle impostazioni che impediscono ai "malintenzionati" di prendere il controllo della webcam o del microfono collegati al PC.

- In aggiunta a un software antivirus, si possono installare anche degli **antimalware** e degli **antispyware**. Soluzioni di questo genere aiutano a individuare e debellare minacce informatiche che potrebbero non essere individuate dagli antivirus e potrebbero quindi penetrare nel PC causando danni fastidiosi e anche importanti Ad esempio, ci sono dei malware che vengono usati per registrare i dati degli utenti e rivenderli a terzi (in questo caso si parla di spyware) e altri malware che, invece, vengono usati per cambiare le impostazioni del browser e dirottare l'utente verso siti pieni di pubblicità (i cosiddetti browser hijacker).

- Attivare o installare un **firewall** è un altro modo per proteggere il proprio PC dalle minacce informatiche. Il firewall è che un sistema di protezione (che può essere sia di tipo software che hardware) posto a protezione di due reti differenti, così da impedire accessi non autorizzati.
- Windows e macOS integrano un firewall volendo, è possibile ricorrere anche a firewall di terze parti, come Windows Firewall Notifier per Windows e Little Snitch per macOS, grazie ai quali estendere le funzionalità di quelli presenti di default sul PC e facilitare il monitoraggio delle attività di rete.

- **Backup:** Eseguire periodicamente dei backup dei lavori eseguiti a pc. In alcuni PC vie l'opzione perché ciò avvenga automaticamente (in macOS Time machine).

- **Aggiornamento di sistema:** è importante tenere aggiornato il sistema operativo del proprio PC, operazione da effettuare periodicamente secondo gli avvisi del sistema stesso.

- **Estensione dei file:** attenzione ai file di **provenienza nota e sicura** con estensioni TAR ZIP, GZ,EXE, DMG e RAR, è sconsigliata l'apertura di questi file.

Videoconferenze e chat audio: si consiglia di impostare le preferenze sull'opzione di attivazione manuale del microfono e della videocamera all'avvio della sessione.

S&L
SALUTE E SICUREZZA
NEI LUOGHI DI LAVORO

Via G. Bovini 41 – 48123 Ravenna (RA) Tel. 0544 465497 333 1182307
www.sicurezzaoggi.com info@sicurezzaoggi.com

ISO 9001:2015

• **Email indesiderate:** evitare di aprire e-mail di dubbia provenienza, soprattutto quelle che sono state smistate automaticamente nelle cartelle di spam/indesiderata, che quasi sicuramente contengono un potenziale pericolo.

• **Phishing:** è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente o persona affidabile in una comunicazione digitale.

• **Documenti non sicuri:** i documenti Word o Excel possono essere veicolo di frode se non utilizziamo alcune precauzioni prima dell'apertura degli stessi. La richiesta all'apertura dell'attivazione delle macro potrebbe creare problemi, perché queste funzionalità agiscono come dei veri e propri programmi e l'utente, qualora le attivi, potrebbe essere oggetto di frode. Abilitare i contenuti **macro,** solo se i file sono di provenienza sicura. La non attivazione porterebbe in molti casi al mancato funzionamento o leggibilità del documento.

• **Installare software provenienti da fonti attendibili:** è buona prassi evitare di installare software di qualsiasi natura, senza che ci sia una richiesta specifica da parte del fornitore di servizi informatici dell'amministrazione o del datore di lavoro. Vuoi evitare di cadere in un simile errore? In tal caso evita di scaricare programmi da fonti poco attendibili e, se possibile, prediligi quelli che sono pubblicati negli store di Microsoft ed Apple, dal momento che prima di essere messi a disposizione per il download, vengono sottoposti a processi di analisi molto severi. Un altro accorgimento che ti consiglio di mettere in pratica è quello di **scaricare software da fonti attendibili**. Virus e malware, infatti, spesso vengono scaricati dagli utenti insieme a dei software che apparentemente sembrano innocui.

• **Password:** Utilizzare password complesse e diversificate per servizi che riguardano la sfera privata o quella lavorativa; disconnettere il computer quando ci si allontana da esso per evitare che altre persone possano accedere ad informazioni sensibili senza il nostro controllo.

• **Evitare di connetterti a reti Wi-Fi pubbliche**: possono non essere adeguatamente protette, e possono essere raccolti dai "malintenzionati" i dati di coloro che vi sono collegati.

Se vi è la necessità di connetterti a Internet quando sei fuori casa, può essere utilizzato lo smartphone come modem. Chiaramente, per navigare in tethering o modalità hotspot, occorre avere a disposizione una SIM con un piano dati adeguato, specialmente se si prevedono molte ore di navigazione o l'utilizzo di molti dati, come ad esempio per guardare contenuti multimediali o scaricare file di grosse dimensioni.

INFO: T.0544 465497. M. 333 1182307 info@sicurezzaoggi.com

Cordiali saluti e Buon lavoro

S&L srl
Mario Padroni