



Decalogo di Sicurezza informatica nello Smart Working



EcoGeo S.r.l.
Sicurezza Ambiente
Qualità Territorio

- ☎ • 0521 773620
- ✉ • info@ecogeo.it
- 🌐 • www.ecogeo.it

In questo periodo vista la crescente esigenza di lavoro da casa, occorre prestare le dovute attenzioni anche agli aspetti di sicurezza informatica. Normalmente la cybersecurity in ambito lavorativo è seguita direttamente dal responsabile interno del settore IT, mentre a casa nostra non sempre abbiamo un livello di attenzione e sicurezza

sufficiente. In particolare se il lavoro da casa prevede che noi trattiamo dati personali sulla base di un'autorizzazione rilasciata dal titolare del trattamento, si dovrà prestare la necessaria attenzione per garantire il rispetto della privacy. In questi casi la prima regola da seguire è quella di chiedere al proprio responsabile informatico come

approntare la propria postazione di lavoro sia che si utilizzi un PC messo a disposizione dall'azienda sia che si utilizzi un proprio device. In affiancamento alle policy aziendali di sicurezza informatica, di seguito proponiamo un decalogo sulle azioni da mettere in atto per operare correttamente.

- 1)** la prima operazione da fare può essere riassunta nel termine "cyber hygiene": si tratta di aggiornare il sistema operativo, ed i software installati sul PC, tramite internet. Tenete sempre aggiornati i vostri sistemi all'ultima versione disponibile, anche abilitando gli aggiornamenti automatici messi a disposizione dai produttori (ad es. Windows Update). Verificate inoltre di avere sempre attivo un antivirus aggiornato. Utilizzate anche un firewall (Windows e Mac sono dotati di un sistema firewall che, anche se non paragonabile ad un sistema specifico dedicato può comunque essere efficace per controllare e bloccare il traffico non richiesto in entrata)





Decalogo di Sicurezza informatica nello Smart Working



EcoGeo S.r.l.

Sicurezza Ambiente
Qualità Territorio



• 0521 773620

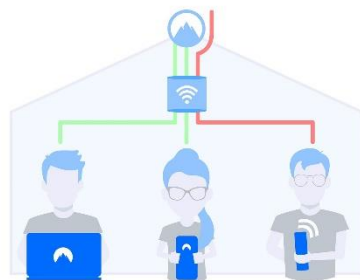


• info@ecogeo.it



• www.ecogeo.it

2) Ogni dispositivo deve avere credenziali di note solo a voi. L'utilizzo di credenziali di autenticazione (login e password) non devono essere condivise con nessun'altra persona, neppure un componente dello stesso nucleo familiare. La password deve contenere lettere maiuscole e minuscole, numeri e simboli speciali combinati in una maniera tale che non risulti comprensibile a un estraneo (esempio: "pA\$\$w03d" non è sicura). 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 anche maggiore rispetto a quanto previsto dalle policy aziendali.



3) Per operare da casa spesso si utilizza la propria connessione internet domestica. E' molto importante in questi casi modificare la password (WPA) del vostro router che vi viene fornita quando fate la prima installazione (normalmente riportata sotto il router stesso). Allo stesso modo per rendere difficile l'individuazione della vostra rete, cambiate anche il nome SSID predefinito della vostra wi-fi (o meglio ancora rendetela non visibile)



Decalogo di Sicurezza informatica nello Smart Working



EcoGeo S.r.l.

Sicurezza Ambiente
Qualità Territorio

- ☎ • 0521 773620
- ✉ • info@ecogeo.it
- 🌐 • www.ecogeo.it

4) Bloccare la postazione di lavoro (tasto Windows + L) ogni qualvolta ci si allontani da essa e ricordatevi di disconnettere eventuali sessioni di lavoro remoto. Configurate anche 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) Per accedere alla rete aziendale da casa è sempre opportuno utilizzare 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 è consigliabile che avvenga 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) Se si lavora su dati personali critici (si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale) è necessario 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.



Decalogo di Sicurezza informatica nello Smart Working



EcoGeo S.r.l.

Sicurezza Ambiente
Qualità Territorio

- ☎ • 0521 773620
- ✉ • info@ecogeo.it
- 🌐 • www.ecogeo.it

7) Qualora l'azienda abbia sottoscritto servizi di Private o Public Cloud Storage (ad es. OneDrive, Google Drive, Box.net, ecc.) verificate 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 quotidiana, sui supporti di memorizzazione prescelti.



8) In caso di smarrimento o furto della postazione di lavoro o dello smartphone è necessario comunicarlo immediatamente all'azienda affinché possa tempestivamente valutare eventuali azioni di protezione dei dati, disabilitare l'account e ove possibile cancellare da remoto i dati contenuti nel dispositivo.



Decalogo di Sicurezza informatica nello Smart Working



EcoGeo S.r.l.
Sicurezza Ambiente
Qualità Territorio

- ☎ • 0521 773620
- ✉ • info@ecogeo.it
- 🌐 • www.ecogeo.it

9) Per ottimizzare la propria configurazione è molto utile utilizzare i software di gestione remota del PC , i quali consentendo ai tecnici aziendali di collegarsi da remoto per gestire e risolvere i problemi rilevati; presiedere sempre alle sessioni di accesso da remoto e non allontanarsi dal proprio PC sino a quando il tecnico non abbia completato la sessione di assistenza remota.



10) In questo periodo Sfruttando le preoccupazioni che il Coronavirus sta generando tra le persone, i criminali del web stanno approfittando di questo momento di vulnerabilità per colpire le ignare vittime con attività di Phishing legate al COVID-19. Diffidate dai messaggi sospetti, evitate accuratamente di aprire gli allegati che essi contengono e segnalate eventuali tentativi di Phishing. Per informazioni ed aggiornamenti seguite il sito della Polizia Postale alla pagina

<https://www.commissariatodips.it/>

Se proprio non potete farne a meno di aprire un file sospetto o visitare un link su cui avete dubbi, potete inviarlo a una sandbox, cioè a un servizio online (ad esempio, Virus Total offre l'analisi gratuita di files e/o URLs per individuare virus o malwares) per farlo analizzare e assicurarvi che sia innocuo.