the i Engineering

# STRUMENTI E SUGGERIMENTI PER UNO SMART WORKING EFFICIENTE E SICURO.

I migliori programmi per la gestione del lavoro e le videochiamate, suggerimenti per dipendenti e titolari e indicazioni per lavorare in sicurezza.

# Introduzione

Moltissime aziende e governi, su scala globale, hanno dovuto adottare misure restrittive per proteggere la salute dei dipendenti e collaboratori e femare la propagazione del contagio da covid19. Molte di queste aziende hanno la possibilità però di fare adottare ai propri dipendenti la modalità smartworking, ovvero il lavoro a distanza da casa. Soprattutto in Italia, dove la cultura dello smartworking è ancora pressochè inesistente, questo implica un necessario cambio di modello sia nella gestione aziendale, sia nel lavoro da parte dei dipendenti. Quali strumenti adottare, quali le precauzioni per la sicurezza e quali i comportamenti migliori.

Dipendenti e collaboratori si collegano ai siti aziendali, partecipano a riunioni in videochiamata e accedono ai dati sensibili dell'azienda via internet, in molti casi attraverso i loro computer di casa e i telefoni cellulari privati.

Sono molti gli strumenti digitali che offrono un eccellente supporto per i lavoratori a distanza, ecco quelli che consigliamo.

## Programmi da utilizzare per lo smart working

Documentare, annunciare e prevedere riunioni a distanza, collaborazione digitale e condivisione di file. Piattaforme ben conosciute come  Skype, GSuite, Slack consentiranno riunioni sicure e gestione affidabile dei file, ma gli utenti devono essere formati e informati.

Alcuni programmi permettono di lavorare in maniera agile con Chiamate (anche video), condivisione dei file, condivisione dello schermo e chat.

1. GSuite / Google Drive
2. Slack
3. Microsoft Teams
4. Skype

# Piattaforme

## GSuite

GSuite è l'ambiente business di Google, una suite di software e strumenti di produttività che consentono di archiviare file in cloud, collaborare con colleghi e collaboratori, creare e modificare file. Include le diffuse applicazioni Web di Google tra cui Gmail, Google Drive, Google Hangouts, Google Calendar e Google Documenti.

Con Google Hangouts puoi conversare con più persone contemporaneamente.

Le conversazioni possono comprendere fino a 150 persone e le videochiamate possono includere fino a 10 persone (Gmail, G Suite Basic) o fino a 25 persone (Business, Education).

Google Drive consente di creare, archiviare e gestire file e documenti in modo collaborativo. Fate attenzione alla condivisione dei file su Google, controllate sempre chi può avere accesso ad essi. Ci sono infatti diversi livelli di autorizzazione, si possono condividere i file a persone specifiche, a utenti che fanno parte della suite aziendale, oppure creare dei link che rendono i file visibili a chiunque possieda il link o addirittura a chiunque nel web, questi sono i più pericolosi, in quanto possono finire nelle mani di malintenzionati.

## Slack

In THE I abbiamo scelto Slack, questo ci permette di collaborare in maniera agile condividendo file, chat, tutto organizzato tramite canali tematici per dividere la tipologia di discussione (un po' come le cartelle email).

Con Slack è possibile utilizzare e collegare diverse applicazioni, da Google Drive per la condivisione di File ai social network. È possibile avviare videochiamate di gruppo ed è possibile creare dei canali tematici in base ai filoni di discussione, per esempio: Canale marketing, Canale agenti, Canale IT. Si possono inoltre includere Bot, webhook e collegamenti ad applicazioni di terze parti (ad es. Google Drive).

## Microsoft Teams

Microsoft teams è l'hub per il lavoro in team di Office 365 che unisce messaggistica istantanea, videoconferenze, chiamate e collaborazione ai documenti. Permette di organizzare riunioni con team fino a 10.000 persone, di organizzare conferenze audio, video e Web con chiunque, all'interno o all'esterno della tua organizzazione. Consente di accedere, condividere e modificare documenti Word, PowerPoint e file Excel in tempo reale.

# Piattaforme

## Skype

Skype è ideale per le piccole imprese di un massimo di 20 dipendenti. È possibile usarla gratuitamente, a meno che non si voglia acquistare credito per effettuare chiamate a telefoni fissi e dispositivi mobili.

Skype for business consente di aggiungere fino a 250 persone alle riunioni online, offre sicurezza a livello aziendale, consente di gestire gli account dei dipendenti ed è integrata nelle app di Office. Microsoft teams sta sostituendo Skype for business.

## Zoom

Zoom è un software che combina videoconferenza, riunioni online, chat e collaborazione mobile. Il piano gratuito consente la partecipazione di 100 partecipanti ma per videochiamate di massimo 40 minuti. Con i piani a pagamento si aggiungono invece diverse funzioni. Zoom si può installare su qualunque dispositivo, ma è possibile accedere anche direttamente dal browser se lo si utilizza sul computer, o scaricando l'applicazione per mobile. In Italia in questo periodo è particolarmente in voga e viene utilizzata soprattutto da insegnanti per le lezioni online.
THE I non consiglia però l'utilizzo di questo software in quanto è stato di recente oggetto di numerose ricerche che hanno individuato numerose falle di sicurezza.

## Io Resto A Casa - iorestoacasa.work

Chiudiamo con un bellissimo progetto italiano. Nato per supportare chi non ha molta familiarità con lo smartworking. Questo progetto si appoggia a Jitsi Meet e Multiparty-Meeting, due progetti Open Source che permettono di effettuare videochiamate semplicemente aprendo un URL tramite browser, senza installare programmi, senza registrarsi. Stanno sperimentando Multiparty-Meeting oltre a Jitsi perché ottimizza l'utilizzo di banda, che in questi giorni è particolarmente sotto stress.

# Suggertimenti per titolari e dipendenti

## Titolari

1. Fidarsi dei propri dipendenti e/o collaboratori è la base per avere una serena e proficua relazione lavorativa: evitare categoricamente comportamenti di controllo ossessivo tipo appello scolastico, verifica status su software di messaggistica.
2. Garantire flessibilità negli orari: non è strettamente necessario che l'orario di lavoro sia statico come quando si lavora in ufficio.
3. Lavorare per obiettivi e non su base oraria.
4. Incentivare lo scambio di informazioni e collaborazione mediante tecnologie adeguate.
5. Evitare di riempire la giornata degli altri con meeting non necessari: email e messaggi via chat spesso sono più che sufficienti.

## Dipendenti

Lavorare da casa non è semplice, soprattutto all'inizio, ma bastano pochi piccoli accorgimenti per rendere tutto più semplice:

1. Lavorare quanto più possibile dalla stessa postazione (ad esempio una cameretta con una scrivania)
2. Non lavorare sul tavolo della cucina o nelle camere da letto (entrambe sono stanze dove ci rilassiamo o condividiamo del tempo con la famiglia, se ci mettessimo a lavorare rischieremmo di mischiare troppo la vita familiare con quella lavorativa)
3. Routine quotidiana: Da quando ci si sveglia a quando si torna a casa dall'ufficio tutti noi seguiamo una routine, è bene portare questa routine anche a casa per separare bene le ore di lavoro con quelle da dedicare ad altro. Quindi, come per andare in ufficio la mattina, colazione e ci si veste, lavorare con il pigiama non aiuta alla giusta separazione lavoro/famiglia, quindi anche se ci si mette una tuta è molto importante vestirsi. Pausa pranzo e poi si ritorna al lavoro. Inoltre consigliamo di fare esercizio fisico di tanto in tanto, alzarsi, cambiare aria e riposare gli occhi.

# Suggerimenti per la sicurezza

**Lo smartworking può avere serie implicazioni impreviste per l'IT e la sicurezza informatica. La vostra azienda è adeguatamente preparata a livello di cybersecurity?**

In questo periodo di emergenza sono molti gli studi che pongono particolare attenzione alle campagne phishing che con la scusa del COVID19 vengono diffuse e cliccate con più facilità, considerate le implicazioni del fatto che i vostri collaboratori clicchino su un annuncio che promette informazioni sulla diffusione del COVID19, o un farmaco miracoloso, ed invece contengono un software progettato per compromettere la sicurezza.

Anche attacchi di ingegneria sociale non sono improbabili, più è grande l'azienda maggiori sono le possibilità che un dipendente venga manipolato da un cybercriminale che dichiara di provenire da un team interno all'azienda.

La vostra azienda gestisce con le adeguate autorizzazioni l'accesso alle password da parte dei dipendenti relative per esempio a sistemi di pagamento, registri del personale, dati personali dei clienti, proprietà intellettuale e altri dati importanti?

Esortiamo le aziende ad implementare una serie di misure pratiche di formazione e tecnologiche, per evitare di aggiungere a questa crisi anche una crisi informatica.

Quando si lavora da casa è necessario adottare più accorgimenti perché subentrano nell'infrastruttura informatica aziendale elementi esterni: tablet, telefoni, computer personali.

A questo proposito vi consigliamo un articolo ben approfondito del Boston Consulting Group sull'argomento, di cui riassumiamo di seguito i 7 punti principali.

**1. Le aziende devono valutare tre categorie di infrastrutture:**

**Endpoint:** Assicurarsi che questi includano applicazioni approvate e strumenti di cybersecurity. Raccogliere un inventario completo dei dispositivi autorizzati a connettersi ai sistemi aziendali, prestando particolare attenzione ai MAC Address dei dispositivi per correlare i dispositivi autorizzati con gli utenti autorizzati (NAC).

**Connettività:** Garantire che le connessioni alle reti aziendali avvengano su reti private virtuali (VPN) con multi factor authentication per evitare lo spionaggio dei dati trasmessi tra gli endpoint dei dipendenti e i server aziendali.

**Architettura e infrastruttura aziendale:** Configurare firewall, reti, strumenti di collaborazione e server per accettare connessioni remote sicure da Internet. La capacità di connessioni remote in molte aziende potrebbe non essere sufficiente per accogliere l'aumento del carico di migliaia di lavoratori connessi. Potrebbe quindi essere necessario acquistare hardware aggiuntivo per i sistemi on-premises o passare rapidamente a un fornitore di servizi cloud.

# Suggerimenti per la sicurezza

## 2. Applicazioni e dispositivi sicuri

La sola infrastruttura IT non garantisce che i sistemi, il software e la sicurezza di un'azienda siano correttamente configurati e funzionino bene.

Crittografare e installare firewall su tutti i dispositivi. Chiedete agli utenti di installare le patch di sicurezza e di aggiornare il software di protezione e sicurezza degli endpoint (EPS). L'EPS fornisce firewall personali, controllo delle applicazioni, antispyware e protezione antivirus, impedendo così agli hacker di accedere a ID e password e di utilizzare i computer come punti di accesso ai server e ai sistemi dell'azienda. Assicurarsi che tutti i dischi rigidi dei computer, i dischi rigidi esterni e le unità USB siano criptati e che l'azienda li rilasci per proteggere gli endpoint dei lavoratori da furti o accessi fisici indesiderati. Preparare delle linee guida per prevenire l'uso di unità USB che non sono state emesse dall'azienda. Tutti gli endpoint dovrebbero essere dotati di funzionalità di cancellazione remota in modo che i dati possano essere cancellati da un dispositivo perso o rubato, così come il software di prevenzione della perdita di dati (DLP) per prevenire l'esfiltrazione di dati. Infine, istruire i dipendenti a eseguire regolarmente il backup dei dati dei laptop sui server aziendali per garantire un rapido recupero dagli incidenti e proteggere i processi aziendali critici.

Accesso sicuro ai sistemi aziendali. Il centro operativo di sicurezza della vostra azienda dovrebbe monitorare tutti i log VPN e di accesso remoto per rilevare eventuali comportamenti anomali. Se l'organizzazione non opera a livello globale, prendere in considerazione la possibilità di limitare l'accesso al sistema a reti o sedi specifiche al fine di ridurre l'esposizione a Internet, mitigare i rischi e garantire il rilevamento tempestivo di comportamenti indesiderati.

Assicuratevi che i processi di risposta agli incidenti informatici siano solidi. Le operazioni di sicurezza e i team IT devono aggiornare e testare tutti i processi e le procedure per garantire che la risposta agli incidenti informatici e le catene di escalation funzionino senza problemi con la forza lavoro remota e il personale di backup. Le aziende dovrebbero anche testare il ripristino dei backup in modo che si possa fare affidamento su di essi durante una crisi.

# Suggerimenti per la sicurezza

### 3. Dev'essere garantita una continuità della SICUREZZA INFORMATICA

Garantire l'accesso di sicurezza in caso di emergenza. Garantire che le operazioni di sicurezza e i team di Incident Response possano accedere ai loro strumenti e collaborare in remoto se non sono in grado di accedere fisicamente ai sistemi o di essere vicini ai colleghi durante un incidente.

Avere un piano di riserva e abilitare il supporto remoto. I piani devono tenere conto della possibilità che almeno una parte del personale di sicurezza informatica contragga il COVID-19 e non sia in grado di lavorare, anche a distanza. Le aziende dovrebbero quindi essere coperte e avere accordi con fornitori di servizi di cybersecurity e IT a distanza e dovrebbero verificare che questi fornitori possano supportare le operazioni a distanza nella misura necessaria.

### 4. Formare i collaboratori sullo smart working e sui rischi annessi

Oltre alle considerazioni tecniche, la formazione sulla sicurezza informatica e le iniziative di sensibilizzazione sono fondamentali per ridurre i rischi. Ecco alcuni dei passi da compiere:

Formare i lavoratori a utilizzare nuovi strumenti e funzionalità in modo sicuro. Assicuratevi che i vostri collaboratori sappiano utilizzare gli strumenti e le tecnologie che supportano la collaborazione a distanza, nonché come riconoscere e prevenire le minacce informatiche. Per ulteriore sicurezza dovrebbero configurare i propri router per creare una rete dedicata ai computer utilizzati per lavoro che sia separata da quella utilizzata dal resto dei dispositivi personali della famiglia.

Stabilire protocolli per l'autenticazione. Istruire i collaboratori a usare solo metodi sicuri per autenticare gli help desk. Il mantenimento di protocolli rigorosi impedirà al personale di divulgare inavvertitamente le informazioni.

Preparare un archivio di informazioni e linee guida. Distribuire materiale come guide self-service, video ed elenchi di domande frequenti che rendano i dipendenti consapevoli delle minacce alla sicurezza e indichino le migliori pratiche per lavorare in remoto in modo sicuro.

Definite esplicitamente le modalità di lavoro a distanza. Fornite linee guida chiare e definite esplicitamente procedure sicure per il lavoro a distanza. Considerare la possibilità di ridurre al minimo l'accesso ai dati solo a coloro che ne hanno bisogno, e allinearsi su orari di lavoro "definiti", questo faciliterà la capacità del team di sicurezza di rilevare attività anomale. Definire la chiusura dell'attività, la fine della giornata e gli altri orari dopo i quali non è più possibile accedere ai dati sensibili, proprio come se i lavoratori uscissero dall'ufficio per andare a casa.

# Suggerimenti per la sicurezza

### 5. Aggiornare le misure di accesso e di sicurezza

I dirigenti e coloro che gestiscono dati sensibili, spesso hanno meno familiarità con la tecnologia e i suoi rischi. I team di sicurezza informatica dovrebbero fornire misure di sicurezza aggiornate per ridurre il rischio di compromissione. Attenzione a truffe phishing, telefoniche e via e-mail, in particolare quelli che sostengono di avere legami con organizzazioni sanitarie o di beneficenza.

Attenzione alle e-mail con allegati sospetti, come gli ordini di acquisto e le fatture di fornitori sconosciuti o di persone che si fingono fornitori conosciuti.

Anche le e-mail con indirizzi sconosciuti che sembrano legittimi devono essere trattate con cautela. La differenza tra i due indirizzi seguenti, ad esempio, è impossibile da rilevare: mail@example.com e mail@example.com. Ma nel primo, la "l" è minuscola, mentre nel secondo, la "l" è stata sostituita da una "I" maiuscola.

Le tecnologie, gli strumenti digitali e le procedure necessarie per proteggersi e diminuire la minaccia cyber sono disponibili e possono essere implementate senza troppi sforzi e spese.

**Noi vi consigliamo di prestare attenzione a questi aspetti, perché anche in campo informatico prevenire è molto meglio che curare.**

Speriamo che questa breve guida possa contribuire a migliorare la conoscenza degli aspetti pratici e di sicurezza dello smart working nell'ambiente aziendale Italiano. Per approfondimenti sugli aspetti relativi alla sicurezza vi consigliamo questa guida ben strutturata e l'articolo a cui abbiamo fatto riferimento:

https://www.ictsecuritymagazine.com/smart-working-e-cyber-security/

https://www.bcg.com/publications/2020/covid-remote-work-cyber-security.aspx

Il team **The I** è disponibile ad una prima valutazione e consulenza in videocall  di 1 ora gratuita, ti raccomandiamo di prenotare il prima possibile perché non possiamo garantire più di 1 consulenza al giorno.

Puoi prenotare chiamando il numero 0445 1888631

Oppure scrivendo una mail a info@thei.it

thei.it
facebook.com/thei.it
twitter.com/thei_it
linkedin.com/company/thei