UNIVERSITÀ DEGLI STUDI DI MILANO
DIREZIONE ICT

*UNIMI 2.0*

# LAPTOP E LAVORO REMOTO IN MODALITA' SICURA

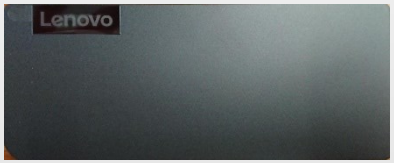
# DOTAZIONE

## Laptop

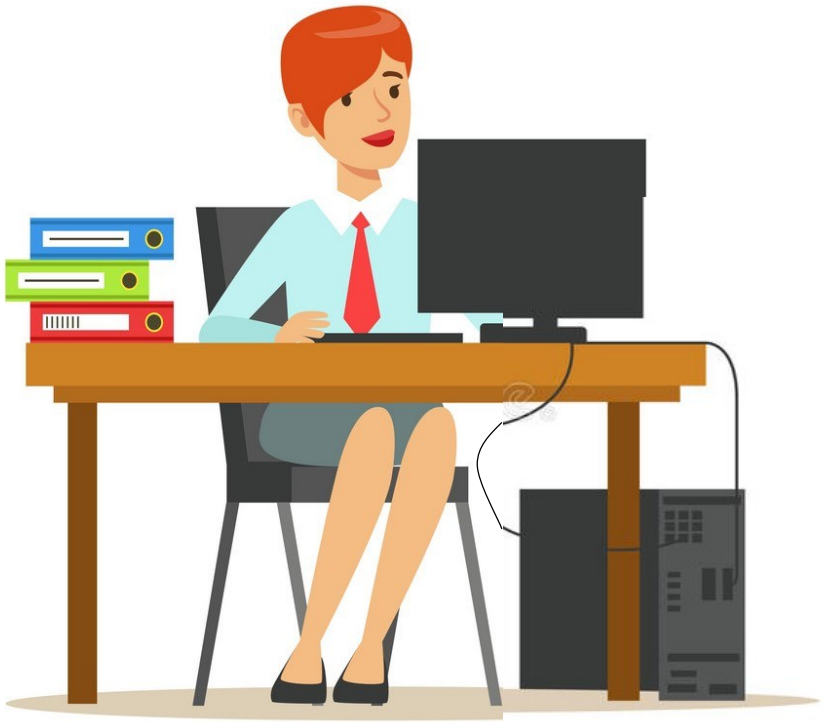
## Lock cable

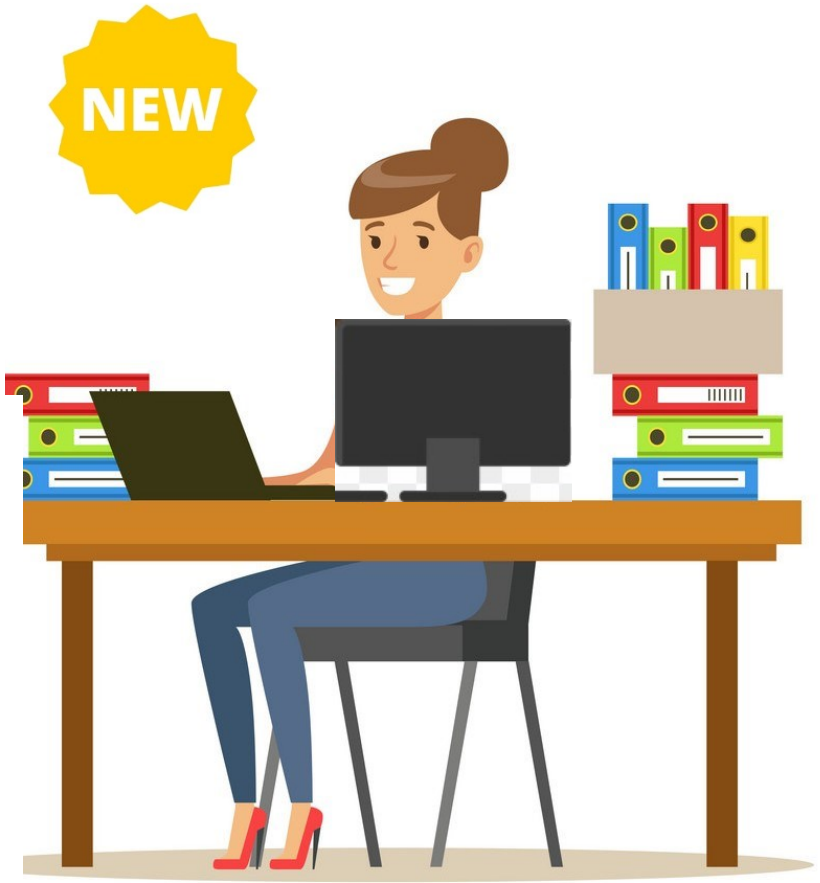
- monitor da -
- cpu c - 10th Gen -
- di ram -
- hd ssd -
- Sophos antivirus –
- pacchetto Office -
- Adobe Reader
- 7zip chrome e firefox -

## Hub multiporta station



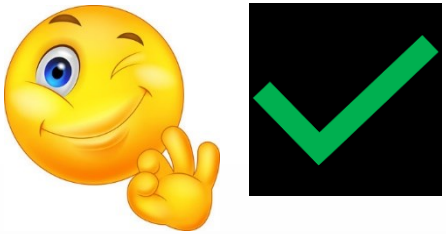
# IN UFFICIO…

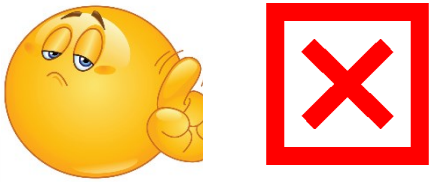




# … A CASA

# 1.500 laptop per svolgere le **attività lavorative**






# SUGGERIMENTI

Il laptop deve essere utilizzato con cura e diligenza

# SUGGERIMENTI

## Prima dell'utilizzo del laptop, agganciare il lock


# SUGGERIMENTI

Durante la giornata, in caso di allontamento:

Bloccare il portatile con il lock, se non lo si è già fatto

Step 1

Bloccare lo schermo del pc

Step 2

Chiudere a chiave l'ufficio

Step 3

# SUGGERIMENTI

Al termine dell'utilizzo:

1) Disconnettersi da tutti gli applicativi e spegnere il laptop

2) Chiudere a chiave il laptop in una cassettiera o in un armadio; oppure, se non disponibili, lasciarlo ancorato e opportunamente celato

3) Chiudere a chiave l'ufficio

# BUONE NORME

1) L'ultimo chiude la porta

2) Massima attenzione durante gli spostamenti


3) Un locale pubblico non è l'ufficio (attenzione a occhi e orecchi indiscreti!)

# LAVORARE DA REMOTO
# IN MODO SICURO IN 15 PUNTI

1. Utilizza le risorse messe a disposizione dall'Ateneo solo ed esclusivamente per lo svolgimento delle mansioni lavorative
2. Accertati di usare sempre la VPN fornita dall'Università
3. Configura una buona password sul router Wi-Fi di casa, per garantire che il tuo traffico non possa essere intercettato facilmente
4. Utilizza delle password robuste (lunghe e complesse) e differenziate per i vari servizi, creandone 1 per l'accesso al PC e ai servizi di Unimi e tante password diverse quanti sono i servizi esterni che utilizzi.
5. Utilizza il profilo di accesso al pc dedicato al lavoro protetto da una credenziale robusta e imposta il blocco del computer quando ti allontani dalla postazione

# LAVORARE DA REMOTO
# IN MODO SICURO IN 15 PUNTI

6. Utilizza sempre l'Antivirus fornito dall'Ateneo (Sophos) e verifica il suo costante funzionamento
7. Non collegare dispositivi esterni (penna USB, Hard Disk esterni) di cui non conosci la provenienza
8. Effettua sempre il log out dai Servizi/Portali di Ateneo
9. Usa sistemi operativi e software aggiornati all'ultima versione disponibile, evitando di installare programmi non più aggiornabili; non installare software provenienti da fonti non ufficiali, in particolare programmi, software o file che violino la licenza d'uso, illegali o modificati illegalmente
10. Presta attenzione quando leggi le e-mail, evita di scaricare allegati o cliccare su link ricevuti in e-mail da mittenti sconosciuti. Evita di usare la casella di posta come archivio di dati. Non impostare inoltri automatici della posta di Ateneo su servizi di posta esterni (ad es. Gmail, …).

# LAVORARE DA REMOTO
# IN MODO SICURO IN 15 PUNTI

11. Per salvare e/o condividere dati, utilizza sempre gli strumenti di Ateneo (ad es. Unimibox, Dataserver, ecc.), che garantiscono maggior affidabilità oltre che il backup dei dati. Non salvare documenti in archivi personali o su risorse cloud non autorizzate espressamente dall'Ateneo
12. Come strumento per riunioni e meeting prediligi Microsoft Teams
13. Presta attenzione durante la navigazione in Internet, evitando siti sconosciuti e rischiosi
14. Usa sempre un atteggiamento cauto e prudente e non rivelare mai informazioni riservate
15. Se ritieni di aver subito un incidente informatico (ad es. allarme antivirus che segnali un software pericoloso; apertura erronea di allegati di una mail insidiosa), comunica l'accaduto con una mail a sicurezza@unimi.it; se nell'incidente sospetti anche una violazione di dati personali, scrivi a violazione.dati@unimi.it

Ulteriori informazioni: https://work.unimi.it/servizi/security_gdpr/118582.htm

# IN CASO DI FURTO O SMARRIMENTO

1 - modifica **immediatamente** password di accesso di Atene
- scrivi a *violazione.dati@ur*

2 Recati a denunciare l'accaduto alle competenti forze dell'ordine entro 15gg o entro 72 ore in caso di furto con destrezza

3 Scrivi a *violazione.dati@unimi.it* allegando la denuncia, anche ai fini dell'attivazione della polizza assicurativa d'Ateneo