

CYBER SECURITY TIPS #41

COME PROTEGGERTI DAGLI HACKER IN CALL?*



LEGGI SUBITO LE NOSTRE TIPS!



*Dalle indicazioni del National Institute of Standards and Technology

1. SEGUI LE REGOLE.

Se la tua azienda ha stabilito una **procedura** a cui attenersi nello svolgimento delle conferenze da remoto, seguila sempre!

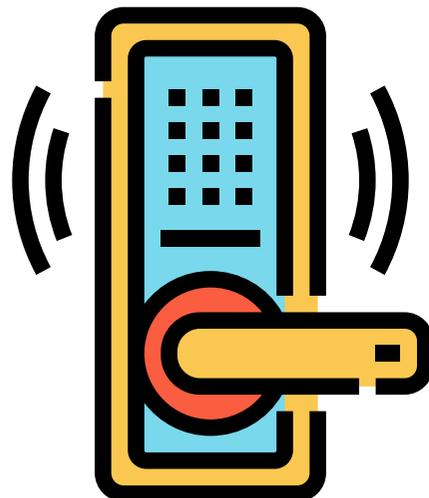
Ti garantirai privacy e sicurezza, inoltre ti svincolerai da responsabilità personali in caso di incidente.



2. NON TUTTI SONO I BENVENUTI!

Se sei l'host, imposta un pin o una **password** per proteggere l'accesso al meeting e limitane il riuso.

Considera infatti che più volte userai lo stesso codice, meno sicuro sarà!



3. FATTI ATTENDERE.

Predisponi la **sala d'attesa** virtuale per controllare i partecipanti e ammetterli alla riunione.

In questo modo ti assicurerei anche che il meeting non parta senza l'host.



4. ANNUNCIA GLI OSPITI.

Fai in modo che tutti gli ospiti vengano annunciati da una **notifica** per poterti accorgere di eventuali "imbucati".
Se questo non è possibile assicurati che l'host (se non sei tu) verifichi l'identità di ogni nuovo arrivato.



5. REGISTRARE? MEGLIO DI NO!

A meno che non sia proprio necessario, evita di **registrare** la call, soprattutto se vengono discusse informazioni strategiche o condivisi dati riservati.



6. MANTIENI IL CONTROLLO (DEGLI SCHERMI).

Limita il numero di persone che possono condividere il proprio schermo e ribadisci a coloro che sono stati autorizzati di non mostrare mai **informazioni sensibili.**



7. TU NON PUOI PASSARE!

Citando Gandalf, ti consigliamo, se possibile, di disattivare le chat così da prevenire il trasferimento di file e link. Anche se conosci tutti i partecipanti alla call, qualcuno potrebbe inviare, senza volerlo, un **malware** o un link malevolo.



TI È STATO UTILE QUESTO POST?



Faccelo sapere
con un like!

lumit.it