PILLOLE DI CYBER SECURITY #2

LE BEST PRACTICE PER PROTEGGERE I DATI A CASA.

CREA UN AMBIENTE D'UFFICIO DOMESTICO SICURO E PROTETTO

1. NON MEMORIZZARE INFORMAZIONI SENSIBILI SU DISPOSITIVI PORTATILI.

- È molto più probabile che i dati vengano persi o rubati se archiviati su un dispositivo portatile.

- Se le tue azioni compromettono segreti commerciali, dati finanziari o proprietà intellettuali, il tuo datore di lavoro potrebbe perdere milioni e tu potresti perdere il lavoro.

- Le informazioni riservate devono restare in ufficio, oppure vi si può accedere da remoto mediante server aziendali sicuri.

LumIT
You Believe
We Create IT

2. NON UTILIZZARE SOLUZIONI DI CONDIVISIONE DI FILE NON AUTORIZZATE SUI TUOI DISPOSITIVI.

- Le soluzioni di condivisione dei file, come le applicazioni per l'archiviazione su cloud e le reti peer-to-peer private, comportano rischi significativi per la sicurezza.

- Non installare mai software non approvati né utilizzare applicazioni non autorizzate sui dispositivi aziendali.

- Non abilitare la condivisione di file sul tuo computer se non consigliato dal reparto informatico.

LumIT
You Believe
We Create IT

3. NON PERMETTERE AD AMICI O FAMILIARI DI USARE I TUOI DISPOSITIVI AZIENDALI.

- Consentire agli amici di utilizzare il proprio portatile di lavoro per leggere le e-mail o lasciare che i figli giochino sullo smartphone aziendale rende i dispositivi vulnerabili.

- Sei responsabile della sicurezza dei dispositivi aziendali e dei dati in essi conservati.

LumIT
You Believe
We Create IT

4. ANCHE I BACKUP PROTEGGONO I DATI

- I backup garantiscono che l'integrità dei dati non sia compromessa e che i dati possano essere ripristinati quando necessario.

- Rispettare le politiche dell'organizzazione sui backup e sul recupero.

- Discutere con il reparto informatico sull'uso di metodi di backup approvati dall'azienda

LumIT
You Believe
We Create IT

TI È STATO UTILE QUESTO POST?

Sharing is
Caring

lumit.it