



6 CONSIGLI PER LAVORARE DA CASA IN SICUREZZA



ATTENZIONE ALLE MAIL DI PHISHING

Il numero di cyber criminali che provano a spacciarsi per clienti conosciuti o colleghi di lavoro, nel tentativo di indurvi a cliccare su link o allegati malevoli, è in continuo aumento.



UTILIZZA PASSWORD COMPLESSE E UNIVOCHE

Evita di utilizzare password facili da decifrare e, per mitigare i rischi, evita di utilizzare la stessa password per tutte le applicazioni.



NON USARE RETI WI-FI PUBBLICHE

Spesso sono gratuite e non richiedono alcuna autenticazione per essere utilizzate, ecco perchè per i malintenzionati è più semplice accedere ai dispositivi collegati a queste reti non protette e non crittografate.



ATTENZIONE AL SOFTWARE ANTI-VIRUS

È importante che l'antivirus sia sempre aggiornato, in questo modo puoi impedire che le vulnerabilità già note del software siano sfruttate per infiltrarsi con facilità nel dispositivo che utilizzi.



PROTEGGI IL WI-FI DI CASA

Il router di casa è di solito configurato con un nome di rete e una password assegnata dal produttore, per ridurre le possibilità di attacco è quindi fondamentale modificarla.

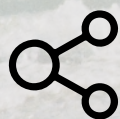


USA UN'AUTENTICAZIONE FORTE

È un ulteriore livello di difesa nel proteggere la sicurezza degli account e-mail, in quanto, oltre alla password, viene richiesta una seconda informazione per confermare la propria identità.

SMART WORKING IN SMART HOLIDAY

Se il lavoro vi accompagna anche in vacanza, ecco 3 buone regole da ricordare



SOCIAL SHARING

Riflettete prima di condividere informazioni sensibili. Dall'altra parte potrebbe esserci qualcuno che vuole farne un cattivo utilizzo.



CLICK!

Prima di cliccare su link e allegati, agite con consapevolezza. Per un cyber criminale è sufficiente un solo click!



DISPOSITIVI

Per una maggiore sicurezza e riservatezza evitate di usare i dispositivi aziendali per uso personale.