

# Come proteggere l'azienda dall'ufficio e da casa

Sia che lavori in ufficio o da casa, la sicurezza aziendale deve rimanere uno degli obiettivi prioritari. Sebbene questi due ambienti di lavoro possano sembrare molto diversi, è possibile adottare le stesse precauzioni per entrambi. Analizziamo alcune importanti regole sulla sicurezza informatica e come applicarle sia in ufficio sia a casa.

## Utilizzare solo dispositivi sicuri

- È bene ricordare che la sicurezza dei dispositivi è direttamente proporzionale alla sicurezza delle applicazioni installate nei dispositivi stessi. Non installare mai un'applicazione o un plug-in senza aver prima consultato il reparto IT.
- Per lavorare, utilizza solamente i dispositivi aziendali. Se utilizzi un computer personale per lavoro, ti consigliamo di creare un account utente separato con una combinazione unica di nome utente e password.
- Con ottime probabilità, in ufficio è il reparto IT a occuparsi della gestione della sicurezza di rete. Per aumentare la sicurezza della tua rete domestica, scegli una password complessa per il router. Se la tua azienda offre l'accesso a una VPN (rete virtuale privata), connettiti anche a questa rete.

## Proteggere la postazione di lavoro

- Quando lavori in ufficio, presta attenzione alle pratiche di piggybacking e tailgating. Il piggybacking si verifica nel momento in cui qualcuno sostiene di far parte della tua azienda e ti segue in un'area protetta, senza utilizzare un badge o un codice di accesso. Il tailgating si verifica nel momento in cui qualcuno attende la tua entrata o uscita da un'area protetta per intrufolarsi all'interno, approfittando della porta aperta. Diffida di tutte le persone che non conosci e non esitare a chiedere un documento di identificazione.
- Quando lavori da casa, scegli un'area appartata e tranquilla dove nessuno possa vedere le operazioni che svolgi sullo schermo. È necessario proteggere tutte le informazioni sensibili dallo sguardo di chiunque non sia autorizzato, compresi partner, figli e amici.
- Blocca sempre il computer quando ti allontani dalla scrivania. Se lasci il computer sbloccato, chiunque potrebbe usarlo per accedere a dati sensibili, sottrarre le tue credenziali di accesso o perfino installare malware.

## Riflettere prima di fare clic

- Non aprire mai link o allegati provenienti da e-mail che non stavi aspettando. Sebbene possa sembrare che il mittente appartenga a un'azienda reale, l'indirizzo e-mail potrebbe essere oggetto di spoofing.
- Se in un'e-mail ti viene richiesto di accedere a un account o a un servizio online, effettua l'accesso dal browser. Non fare mai clic sul link contenuto nell'e-mail. Se accedi direttamente al sito, potrai avere la certezza di entrare nel sito Web reale anziché in uno fasullo dall'aspetto simile.
- In caso di dubbi, contatta telefonicamente il mittente dell'e-mail per verificare che la richiesta, il link o l'allegato siano legittimi. Non chiamare il numero di telefono indicato nell'e-mail, potrebbe trattarsi di un numero falso.



Il team di sicurezza KnowBe4