Smart Working Resiliente: la necessità di cyber security è anche domestica. Cosa possono fare gli utenti?

1 USA PASSWORD SICURE E DEDICATE AI DISPOSITIVIAZIENDALI

Nelle nostre case coesiste un elevato numero di device connessi alla stessa rete e con protocolli di sicurezza a volte insufficienti.

a) Non riutilizzare la stessa password per account personali e aziendali.
b) Cambia di frequente la password, evitando l'uso di parole comuni, date importanti e informazioni facilmente reperibili online.
c) Usa un password manager per conservare e memorizzare le tue password senza doverle ricordare tutte le volte.

2 USA CONNESSIONI SICURE E AGGIORNATE

Le reti domestiche non sono sempre connessioni sicure e aggiornate.

a) Utilizza la connessione VPN (virtual private network) aziendale.
b) Aggiorna i device con le ultime patch di sicurezza.
c) Evita l'uso promiscuo degli strumenti aziendali, limitando l'utilizzo dei dispositivi lavorativi anche nell'ambito familiare.

3 ATTENTO PUO' ESSERE PHISHING!

Si stanno moltiplicando gli attacchi mirati a sottrarre informazioni, dati personali e password aziendali.

a) Non utilizzare la tua mail personale in ambito lavorativo. Evita di rivelare informazioni finanziarie e commerciali anche sui social network e chat.
b) Diffida di link o mail sospette ed evita di scaricare allegati da mittenti sconosciuti. Prima di cliccare su un link, sposta il cursore sopra di esso e verifica che l'indirizzo sia affidabile.
c) Presta attenzione alle chiamate sospette ricevute da operatori che potrebbero fingersi di essere il supporto tecnico dell'azienda sottraendo informazioni e password.

4 MANTIENITI IN CONTATTO CON IL TUO TEAM PER GARANTIRE UNA RESILIENZA OPERATIVA

Cambiare modalità di relazione con il proprio team di lavoro può disorientare.

a) Non aver paura di "disturbare" il tuo team, non esitare a contattarlo.
b) Organizza almeno un meeting al giorno con il tuo team di lavoro
c) Prediligi l'utilizzo di call e videocall rispetto all'utilizzo di mail e IM (Instant Messaging).

5 FAI REGOLARMENTE IL BACK UP DEI DATI

La sicurezza al 100% non esiste, soprattutto in questo momento di emergenza sanitaria.

a) Effettua e mantieni aggiornata una copia di tutte le attività e di tutti i dati.
b) Fai un back up dei dati: questo ti consente, in caso di attacco andato a buonfine, di ripristinare tempestivamente la tua operatività.