01 BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

02 PASSWORD

Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

03 ANTIVIRUS

Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

04 ALLEGATI

Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

05 SOCIAL ENGINEERING

Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni

06 VPN

Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili

07 CONDIVISIONE

Non usare strumenti di condivisione dati pubblici (es. Wetransfer) ma cloud privati (es. Google Cloud, Azure, DropBox), proteggendo i dati con password robuste

08 CRITTOGRAFIA

Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili

09 PROCEDURE

Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

10 ACCESSI

Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti