# SICUREZZA DELL'INFORMATICA MOBILE

Evita di accedere a siti Web tramite **link** contenuti in messaggi ricevuti ma non richiesti e usa invece l'indirizzo Web corretto, scrivendolo direttamente nella casella del browser.

Negli accessi all'area riservata o ai siti Web che richiedono l'autenticazione, valuta con attenzione la possibilità di salvare **username** e **password** nel browser e nella app.
In particolare, gestisci con prudenza le credenziali che consentono l'accesso a dati sensibili e metodi di pagamento.

Evita di fornire **dati personali** o i dati della carta di credito in risposta a messaggi o email. Nel dubbio, contatta l'azienda o la filiale della banca per verificare l'autenticità della richiesta.

Controlla periodicamente il **credito** telefonico e il traffico mobile, verificando l'eventuale presenza di spese non autorizzate.

Effettua **backup** regolari dei dati importanti contenuti nel dispositivo, per facilitare il ripristino in caso di guasto, furto o smarrimento del dispositivo stesso. Le soluzioni più efficienti si basano normalmente sull'uso di piattaforme cloud e sulla sincronizzazione dei file, specialmente nel caso di gestione di documenti e dati sia tramite PC, sia tramite smartphone o tablet.

Attiva il **codice PIN** (*Personal Identification Number*) per proteggere il dispositivo dall'uso non autorizzato, oppure imposta il riconoscimento facciale o dell'impronta digitale.

Disattiva i servizi di **localizzazione** e **Bluetooth** dell'informatica mobile se non sono indispensabili, perché possono favorire la connessione al dispositivo e ai suoi dati a tua insaputa, oppure l'invio di messaggi e annunci sulla base della località in cui ti trovi. L'attivazione di questi servizi è spesso predefinita nelle impostazioni del dispositivo.