Come proteggere i propri dispositivi?

COMPUTER

- **Proteggi il computer con Antivirus e dispositivi anti-spam** delle mail: installare un programma Antivirus è un buon modo per proteggere il PC da eventuali "virus informatici" provenienti da siti, email, CD masterizzati, chiavette USB e altri dispositivi di archiviazione.

  Ti consigliamo di:
  - effettuare aggiornamenti frequenti sul sito del produttore o attraverso gli aggiornamenti automatici (live update)
  - utilizzare programmi per la gestione della posta elettronica in grado di filtrare le email inviate con scopi illeciti
  - utilizzare dispositivi Firewall per controllare il flusso di informazioni che partono e arrivano al computer. Si possono facilmente scaricare da Internet o acquistare

- **Aggiorna spesso il sistema operativo e il browser**

  Tenere aggiornato il sistema operativo del Pc e il browser rende la navigazione più sicura.
  Le aziende produttrici dei Sistemi Operativi e browser rendono disponibili online e scaricabili gratuitamente, gli aggiornamenti degli stessi, ad eccezione di quelli non più supportati (es. Windows XP). In generale è consigliabile non utilizzare sistemi operativi non più supportati dai produttori.
  Inoltre, a seguito degli aggiornamenti degli standard di sicurezza adottati da Credit-Agricole Italia sui propri servizi online, utilizzando sistemi operativi e browser non aggiornati, l'accesso a tali servizi potrebbe essere bloccato. Ad esempio, l'accesso non è più consentito ai sistemi operativi e ai browser che non supportano il protocollo TLS 1.2

- **Non utilizzare chiavette USB o altri supporti se non sei certo della provenienza** e, nel caso, fai subito una scansione con il programma Antivirus

- **Scarica file solo da fonti attendibili, note e sicure:**

  Condividere o scaricare file su Internet significa lasciare una "porta aperta" a rischio di virus. Particolari software, denominati spyware, possono avere facile accesso e "catturare" via Internet informazioni personali a tua insaputa.
  E' consigliabile utilizzare sempre Antivirus e Firewall e ricorrere solo a fonti attendibili, note e sicure.

DISPOSITIVI MOBILE (SMARTPHONE E TABLET)

- Installa un software di sicurezza (antivirus) e tienilo sempre aggiornato, per evitare infezioni sul dispositivo. Se possibile, installate un'app di mobile security in grado di segnalare se il dispositivo è stato compromesso
- Effettua un backup frequente dei dati e aggiornare regolarmente tutte le vostre app: Effettuando il backup dello smartphone o tablet sarà possibile ripristinare facilmente i dati personali in caso di smarrimento, furto o danneggiamento del dispositivo
- Tieni il Sistema Operativo dello smartphone sempre aggiornato, scaricando gli ultimi aggiornamenti disponibili
- Non lasciare mai il tuo dispositivo incustodito in aree pubbliche
- Evita di acquistare app presso app store di terze parti, ma acquista da quelli ufficiali
- Prima di scaricare un'App fai una ricerca sia sull'app che sugli autori e controllare le recensioni degli altri utenti
- **Verifica le autorizzazioni richieste dall'app**: controlla a quali tipologie di dati può accedere, se può condividere dei dati con soggetti esterni e se è effettivamente necessario che abbia tutte le autorizzazioni richieste.
- Utilizza le funzioni di blocco della schermata di accesso al dispositivo, e cambiare spesso il codice
- Elimina informazioni riservate dal dispositivo prima di qualsiasi intervento di assistenza o manutenzione
- Non custodire informazioni finanziarie (numeri di carte di credito, password di accesso agli store, pin etc.) sul dispositivo
- **Gestisci le "Reti di connessione**" (WIFI, Bluetooth®): non lasciare attive queste connessioni e i servizi di localizzazione quando non utilizzate; utilizza sempre una rete wi-fi protetta per conneterti al sito o all'app mobile
- **Non consentire alle app di utilizzare i servizi di localizzazione**, a meno che non sia strettamente necessario: queste informazioni potrebbero essere condivise ed essere utilizzate per l'invio di annunci basati sulla località.
- Controlla periodicamente il dettaglio del traffico mobile per valutare la presenza di eventuali spese sospette:
- nel caso contattare il gestore telefonico.

IMPORTANTE

Non modificare il dispositivo (root / file system...) né eseguire Jailbreak: effettuando il jailbreak del dispositivo**, la sua sicurezza può essere compromessa in modo significativo e aprire falle a livello di sicurezza che potrebbero non risultare subito evidenti**.