Recentemente il Garante della privacy si è espresso sull'uso di tablet e smartphone a scuola.

Lo ha fatto attraverso un video che illustra una serie di suggerimenti utili per i docenti al fine di non incorrere in violazioni delle norme sulla privacy.

{loadposition user7}

Su Orizzontescuola è disponibile una sintesi di queste raccomandazioni che rilancio per favorirne la massima condivisione.

Le nuove generazioni utilizzano costantemente gli stumenti tecnologici e, in alcune scuole, hanno la possibilità di effettuare delle attività didattiche che prevedano l'uso dei tablet. Inoltre, scattano delle foto durante le lezioni, senza che il docente se ne accorga. Sicuramente è compito del docente vigilare affinché gli studenti non facciano un uso sbagliato degli strumenti informatici, violando costantemente la privacy.

Il Garante per la protezione dei dati personali ha messo insieme nel video di seguito incorporato alcune informazioni utili per tutelare la privacy quando vengono utilizzati smartphone e tablet.

Un primo suggerimento è quello di non conservare mai su questi strumenti delle informazioni eccessivamente riservate, in quanto si assiste non di rado a smarrimenti, furti e clonazioni da parte dei pirati informatici. Tra i dati molto riservati rientrano tutte le password di accesso ai siti vari, codici di accesso, dati bancari, etc. La stessa attenzione va posta anche nei casi in cui

smartphone o tablet vengono donati a terze persone, in quanto spesso le informazioni riservate restano memorizzate a nostra insaputa. Per tale ragione si suggerisce di effettuare il ripristino delle impostazioni iniziali, ossia delle impostazioni presenti sullo strumento al momento dell'acquisto, la rimozione della scheda SIM, la rimozione delle schede di memoria esterna e la rimozione di tutti i backup a mano a mano effettuati e che rimangono memorizzati all'interno dello strumento.

Per proteggere i dati è necessario impostare sempre un codice di accesso al dispositivo elettronico. Questo è un blocco immediato nei confronti di coloro i quali volessero leggere la corrispondenza elettronica, gli sms e tutte le altre informazioni riservate di immediato accesso. Il codice di blocco deve essere comunque complicato, ovvero vanno evitati i nomi semplici, le date di nascita e comunque codici che siano facilmente riconducibili ad elementi in vista della vita del possessore dello strumento.

Va inoltre conservato con cura il codice IMEI del dispositivo. Esso si può reperire nella scatola dello strumento, oppure vi si può risalire mediante le impostazioni. In caso di smarrimento o furto del disposibito, la conoscenza dell'IMEI ne permette il blocco, quindi gli strumenti diventano inutilizzabili.

La navigazione su smartphone e tablet deve sempre essere effettuata dopo aver controllato le impostazioni sulla privacy del dispositivo e le condizioni di utilizzo dei vari servizi. Ogni servizio online consente l'uso dopo un consenso dato per determinati scambi di informazioni che vengono dichiarate dal "contratto", ma che quasi mai vengono lette. Va anche utilizzato sempre un antivirus, per evitare gli attacchi informatici da parte di hacker oppure l'installazione di fastidiosi virus.

Negli spazi che offrono connessione wi-fi free bisogna fare attenzione alle impostazioni di navigazione, in quanto è necessario assicurarsi che la navigazione sia sempre protetta mediante protocolli di scambio dati criptati. Per tale ragione le autenticazioni ai siti devono essere effettuate utilizzando sempre il protocollo Https, che assicura un'elevata sicurezza soprattutto quando si vogliono effettuare operazioni di home banking.

Quando vengono scaricate determinate applicazioni, a volte viene visualizzato un messaggio di avviso relativo alla provenienza sconosciuta dell'applicazione. Per tale ragione non si è sicuri del fatto che ciò che stiamo installando sia garantito ed esente da eventuali problematiche. È quindi necessario scaricare le applicazione dai vari market ufficiali dei dispositivi in uso e, una

volta installate, controllare sempre le richiesto di accesso ai dati personali contenuti nel dispositivo (alcune app chiedono l'accesso alle foto, etc.)

Nel caso in cui si volesse impostare un account e-mail, è bene fare attenzione alle mail di spam che bombardano le caselle di posta elettronica. Molte mail presentano dei link quasi sempre sospetti che invitano a inserire delle credenziali al fine di effettuare clonazioni di vario genere.

In ultimo, ma non meno importante, si ricorda che smartphone e tablet utilizzano delle funzioni di geolocalizzazione. Queste funzioni permettono di inviare la propria posizione immediatamente alla rete, permettendo a diversi utenti, soprattutto dei social network, di sapere dove ci si trova in quel dato istante. Coloro i quali volessero "nascondere" la propria posizione, devono disattivare la funzione di geolocalizzazione dalle impostazioni.

{jcomments on}

{loadposition user6}