La nostra vita si svolge sempre più online, e questo vale soprattutto per i più giovani. Gli studenti, in particolare, non solo navigano su Internet nel loro tempo libero, ma lo fanno anche per studio, su consiglio o richiesta degli insegnanti stessi.

{loadposition user7}

Internet è una fonte inesauribile di informazioni, quindi ovviamente è lo strumento perfetto per approfondire le proprie conoscenze: pertanto, è normale che gli studenti lo utilizzino per fare ricerche, comprendere meglio i concetti spiegati a scuola, ecc. La pandemia da Covid-19 ha poi introdotto una nuova famiglia di strumenti online nella vita degli studenti: per seguire le lezioni a distanza, infatti, era necessario utilizzare app per videochiamate, piattaforme per la condivisione di file, ecc.

Questi strumenti e attività portano gli studenti a condividere molte informazioni online, spesso anche inconsapevolmente, o comunque senza le dovute cautele. E non è solo un problema degli studenti: anche le istituzioni scolastiche e universitarie utilizzano frequentemente strumenti online, condividendo informazioni relative ai propri studenti (ad esempio quando pubblicano contenuti sui canali social).

Condividere informazioni online per alcune attività educative è inevitabile: inviare un compito

al proprio insegnante o seguire una videolezione sono attività che non possono essere ignorate. È però molto importante essere consapevoli dei rischi e mettersi al riparo il più possibile.

Quali sono i rischi?

Parliamo quindi di quali rischi può correre uno studente che condivide informazioni online. I pericoli principali sono due, e riguardano la propria identità reale e quella online. Alcune informazioni potrebbero infatti rivelare a eventuali malintenzionati le credenziali di accesso ai propri account personali; altre informazioni potrebbero invece rivelare l'identità reale dello studente (nome, cognome, indirizzo, ecc.).

Se un malintenzionato dovesse rubare le credenziali di accesso agli account personali dello studente, potrebbe essere in grado di fare molti danni. In primo luogo, avrebbe accesso a moltissime informazioni riservate; inoltre, potrebbe fingersi di essere lo studente in questione e ostacolarne la carriera scolastica o universitaria. Se poi lo studente utilizza lo stesso nome utente e la stessa password per altri account, il truffatore avrebbe accesso anche a quelli.

Se invece il malintenzionato in questione dovesse riuscire a risalire all'identità reale dello studente, e quindi anche al suo indirizzo, potrebbe arrivare persino a minacciare la sua incolumità o comunque cercare di intromettersi nella sua vita di tutti i giorni.

Esistono poi molte altre informazioni, apparentemente di minore importanza, che potrebbero però causare grossi problemi se rivelate a malintenzionati. Ad esempio, informazioni relative alla carriera scolastica potrebbero avvantaggiare o svantaggiare gli studenti nel caso di concorsi, richieste di lavoro, ecc. Dalle scuole e università potrebbero arrivare anche informazioni relative alla salute degli studenti, che potrebbero essere utilizzate per discriminare i meno fortunati.

Difendersi dai rischi della condivisione di informazioni online

Come abbiamo visto, i rischi sono diversi e i potenziali danni molto gravi. Per questo è fondamentale cercare di proteggersi e di tutelare i propri figli più piccoli. Ecco alcuni semplici

consigli per farlo.

1. Non condividere informazioni personali online

Può sembrare banale, ma la regola principale, soprattutto per i più piccoli, dovrebbe essere quella di non condividere informazioni personali online. Non bisogna quindi rivelare il proprio nome e/o indirizzo, e sarebbe meglio non condividere foto personali, soprattutto se permettono di riconoscere dove ci si trova.

2. Usare una VPN

Usare una VPN consente di proteggere la propria connessione a Internet, crittografando il traffico e mascherando il proprio indirizzo IP. In questo modo, le informazioni condivise risulterebbero illeggibili agli hacker che dovessero entrarne in possesso. Alcune VPN, poi, mettono anche a disposizione servizi di sicurezza aggiuntivi, come quelli per la protezione malware .

3. Usare password forti

Per proteggere i propri account personali è fondamentale usare password sicure , quindi contenenti lettere, numeri e caratteri speciali, e uniche, cioè non condivise tra più account diversi. Per evitare di doversele ricordare tutte a memoria, può essere utile impiegare un password manager, in modo da poterle creare e salvare automaticamente.

4. Usare app affidabili

Esistono molte app che permettono di scambiare documenti e messaggi con i compagni di scuola o di università: non tutte sono però affidabili. Se la propria scuola o università dispone di app ufficiali, bisognerebbe usare quelle: generalmente sono pensate anche per proteggere la privacy degli studenti. Se invece è necessario fare ricorso ad app di terze parti, meglio affidarsi

a prodotti ben noti di grandi aziende, che in generale sono in grado di garantire uno standard di sicurezza più elevato.

{jcomments on}

{loadposition user6}