**INFORMATICA & EDUCAZIONE CIVICA**

**LAVORO DI: Di Paoli Nicolò**

In un mondo in cui gli utenti sono sempre più interconnessi tra loro e la presenza sui Social Networks è capillare e continua (sono coinvolti non sono i *millennials* ma ormai quasi tutte le fasce d’età superiori), diventa irrinunciabile **preoccuparsi della propria privacy** e del pericolo di finire in qualche “**truffa online**” o di vedersi **carpire informazioni personali** (dati personali e bancari, password, etc).

Purtroppo ogni giorno veniamo a conoscenza di nuovi casi di **phishing**, di **virus** e trappole messe in atto da **pirati informatici** che possono esporci a grossi rischi. I **social network** sono le piattaforme che più vengono utilizzate per compiere aggiornamenti, soprattutto per svago ma sempre più anche per lavoro per gestire gli account ufficiali delle aziende: sono proprio loro ad essere sotto la lente d’ingrandimento, poiché è **molto facile manometterli**.

A tal proposito, lo scorso 9 febbraio si è svolta la giornata europea del **“Safer Internet Day”** dedicata alla sicurezza in rete dei ragazzi contro il cyberbullismo.

Ecco alcuni consigli per non farsi rubare le informazioni personali:

## **1. SCEGLIERE UNA PASSWORD SICURA**

## **La password è la chiave che apre la porta a tutte le vostre informazioni**. Quanto più sicura è, meno sarà facile per i malintenzionati accedere ai vostri dati. Ricordatevi di non utilizzare la stessa password per diverse piattaforme e di renderla difficile da indovinare, non scontata. Meglio utilizzarne una alfanumerica con caratteri maiuscoli, minuscoli e che contenga anche simboli.

## **2. EFFETTUARE SEMPRE IL LOGOUT DEL VOSTRO ACCOUNT**

## Terminata una sessione internet in cui avete effettuato il login con il vostro account, ricordatevi di **eseguire sempre il logout**, soprattutto se siete fuori casa e non con il vostro pc: qualsiasi persona poco raccomandabile potrebbe accedere ai vostri dati o, nel peggiore dei casi, pubblicare qualcosa sui social network a vostro nome tramite il vostro account.

## **3. ENTRARE SOLO IN SITI WEB SICURI**

## Tutti dovrebbero sapere che esistono due estensioni per i siti internet: la **http://** e la **https://**. Entrambe sono corrette, ma la seconda indica l’**esistenza di sistemi di sicurezza**.

## **4. ATTENZIONE ALLE TRUFFE VIA EMAIL**

Purtroppo questo è uno dei più comuni mezzi di truffa online. Il conosciuto fenomeno del **phishing**, ossia la ricezione di una comunicazione per esempio dalla propria banca che vi avverte di un’anomalia nel vostro conto corrente e vi porta a cliccare un link, è uno dei metodi utilizzati dai truffatori per estorcervi i dati di accesso al vostro conto bancario.

##

## **5. NAVIGARE SICURI TRAMITE MOBILE**

Con lo smartphone (e tablet) è bene fare molta attenzione. Innanzitutto è bene **tutelarsi inserendo un PIN o un codice di sicurezza** per proteggere i propri contenuti da occhi indiscreti. E’ molto importante anche non effettuare il download di applicazioni o giochi pirata: dal dispositivo mobile è molto più facile cadere in qualche tranello senza accorgersene ed è, ahimè, molto più facile anche per i truffatori accedere ai vostri dati, siano essi sms, password o foto. In caso di furto o smarrimento del vostro telefono, se avete attivato il servizio di localizzazioni potete controllare dove si trova e sapere quando è stato utilizzato l’ultima volta. Addirittura può essere fatto squillare o bloccato a distanza.

## **6. SE SI ACQUISTA ONLINE..**

Inutile dirlo, per stare tranquilli, basta effettuare gli acquisti su siti web sicuri, ufficiali e leader del settore. Se per caso voleste acquistare un prodotto su un sito web che non conoscete, il consiglio che vi diamo è quello di controllarne l’**affidabilità online**: tra le varie recensioni e informazioni, troverete sicuramente la risposta che cercate.

## **7. ATTENZIONE CON I SOCIAL NETWORK**

Nessun ambito come quello dei social network è potenzialmente più pericoloso per la diffusione non volontaria dei vostri dati. Girano infatti nelle bacheche e negli stream (flussi) molti link che se cliccati potrebbero portarvi a siti esterni che non c’entrano niente con quello che vi aspettavate. Bisogna fare attenzione anche alle richieste di amicizia da parte di persone che non conoscete, meglio diffidare. In particolar modo per gli adolescenti che accedono è bene fare estrema attenzione che dietro quel profilo non si nasconda un adulto malintenzionato.

## **8. UN OCCHIO DI RIGUARDO PER I BAMBINI**

Abbiamo dedicato un articolo sulla tutela dei minori online. Quasi tutti i sistemi operativi consentono di impostare i parametri di accesso dei bambini alla rete, evitando l’accesso a certi siti web e impostando un tempo massimo di connessione.

## **9. INSTALLARE UN ANTIVIRUS**

## Tutti conoscete cosa sono e a cosa servono. Tuttavia, molto spesso si evita di installarli per pigrizia o perché, comunque, costano. I virus attualmente sono talmente evoluti da insinuarsi sempre più facilmente nei nostri sistemi, anche senza che ce ne si accorga allo scopo di rubare i vostri dati sensibili o comunque di fare danni all’interno del vostro pc.

## **10. EFFETTUARE SEMPRE IL BACKUP**

Fare backup continui e aggiornati di tutti i propri dati è fondamentale. Soprattutto per quanto concerne i dati importanti: esistono gli harddisk e le chiavette usb in cui salvare tutti i vostri file come anche i sistemi di salvataggio su cloud online grazie ai quali salvare ogni documento.