Consigli per usare i social network, da parte della POLIZIA di Stato

- **Proteggere il dispositivo che utilizzate per accedere ad Internet**

Aggiornate costantemente il software che utilizzate per la navigazione su Internet. Usate firewall, antivirus e antispam. Insomma proteggete sempre il dispositivo (computer, smartphone o tablet) che utilizzate per navigare sul web, perché all'interno ci sono dati personali che potrebbero essere usati a vostra insaputa da persone che accedono tramite la rete, ma anche da amici, colleghi e altro. Quindi impostate il blocco automatico quando i dispositivi entrano in stand-by e bloccate lo schermo con password. Cellulari e tablet danno anche la possibilità di impostare pin per la protezione.

- **Proteggere la password**

Proteggete sempre la vostra password, non la divulgate e cambiatela periodicamente (almeno ogni 3 mesi). Utilizzate sempre il numero massimo di caratteri che vi vengono messi a disposizione dal sistema, perché rendete più difficile la violazione da parte dei programmi che decriptano password. Possibilmente non usate parole di senso compiuto, usate combinazioni di minuscole, maiuscole, numeri e caratteri speciali ($@#). Non legatela a parole della vostra vita privata o a date di nascita dei vostri familiari. Cambiate password per ogni account e cambiate subito quella assegnata inizialmente in automatico.

- **Utilizzare reti sicure**

Prestate molta attenzione alle informazioni personali quando accedete ad internet utilizzando una rete che non conoscete o di cui non siete sicuri (ad esempio una rete Wi-Fi gratuita in un locale pubblico). Con queste reti, chiunque nelle vicinanze, con conoscenze informatiche adeguate potrebbe monitorare le informazioni trasmesse tra il computer/ smartphone e l'hotspot Wi-Fi. Inoltre se possedete una rete Wi-Fi a casa, proteggetela con una password per evitare che altre persone la possano violare.

- **Proteggere le informazioni personali**

Prima di inserire i dati personali in un modulo o in una pagina web, verificate la presenza di indicatori che ne attestino la sicurezza (ad esempio che l'indirizzo contenga la scritta ***https*** e il simbolo del lucchetto chiuso

accanto). Per comunicazioni riservate utilizzate software di cifratura per criptare un documento. Così se anche il messaggio venisse intercettato, senza la chiave utilizzata per crittare il documento si avrebbero solo una serie di caratteri privi di significato. Molti programmi su internet sono disponibili gratuitamente per questo tipo di servizio. Nei social e nelle chat non divulgate mai informazioni sensibili come il nome, l'indirizzo, il numero telefonico, il numero di conto o la password

- **Evitare le truffe**

Prima di cliccare su link o documenti allegati ad un messaggio di posta elettronica proveniente da un mittente sconosciuto che vi promette un regalo, un viaggio gratis o qualsiasi altro premio, riflettete! Potrebbero contenere virus o malware in grado di nuocere al vostro dispositivo o addirittura rubare le informazioni personali. Gli antivirus riducono drasticamente i rischi di contagio ma bisogna anche tener presente che se non è aggiornato non riconosce quel file come contenente un virus, poiché anche i virus sono continuamente aggiornati per violare i sistemi di sicurezza. Per gli acquisti online, fate prima ricerche sul venditore. Se un'offerta appare troppo conveniente per essere vera, potrebbe nascondere una brutta sorpresa. È meglio acquistare prodotti solo da siti sicuri, certificati e con recensioni positive.

- **Prevenire il furto di identità**

Non vi fidate di messaggi o siti che chiedono dati personali o finanziari e ripeto non inviate le password tramite posta elettronica, e soprattutto non condividetele con altre persone.

- **Usare i social network con prudenza e rispetto**

Nei profili personali dei Social network limitate la visione dei contenuti (dati, foto, ecc..) solo a persone fidate, utilizzando le opzioni sulla privacy. Prestate sempre attenzione nel pubblicare video, foto o post con informazioni personali, potrebbero essere diffuse in modo "virale" e potreste pentirvene.

- **Non rispondere alle provocazioni**

Quando ricevete mail, chat o sms provocatori e/o minacciosi, evitate di rispondere ed in caso di insistenza bloccate o segnalate il contatto che vi infastidisce. Spesso chi utilizza la rete in questo modo, sono i cosiddetti Cyberbulli e Cyberstalker.

- **Segnalare i contenuti illeciti o inappropriati**

Segnalate i contenuti illeciti o inappropriati che trovate su Internet e che a vostro parere violano le norme della community, per consentire di esaminarli, di difendersi e per garantire una esperienza di navigazione online migliore per tutti.

- **In caso siate vittime di gravi reati telematici, potete fare la denuncia nel posto di Polizia più vicino o attraverso il Commissariato di PS online.**

(aggiornamento ottobre 2016)