



La cyber security nelle scuole

Continuano a crescere i pericoli per i minori - bambini, ragazzi - online, su internet: sul web, nelle chat e nei social. Beninteso, è riconosciuto che l'interazione con gli strumenti elettronici apporti una serie di benefici per lo sviluppo dei bambini più piccoli, in quanto costituisce un'occasione per **imparare rapidamente divertendosi**.

Essere adulti online non è semplice; ancor meno lo è per i minori, sovraesposti e bombardati sotto ogni fronte, sia che si tratti di pedofilia sia che si tratti di tecniche di marketing borderline. Per tali ragioni è sempre più importante, data la rilevanza che la tecnologia e il web hanno assunto anche

nella quotidianità dei più piccoli, essere presenti, condividere i momenti che si passano dinanzi allo schermo e educare i ragazzi sin da piccoli ad un sano utilizzo dei sistemi digitali, fornendo loro gli strumenti conoscitivi per comprendere e prevenire ogni situazione di rischio, pur nei limiti delle loro capacità.

I rischi più gravi, diciamoli subito, sono forse due:

- Il rischio di **assuefazione ed interdipendenza da contenuti di scarsa qualità**:
- Il rischio di **finire vittima di predatori sessuali**: nuove tecnologie e nuovi servizi comportano, infatti, nuove tecniche di adescamento nei confronti dei minori, con il rischio di essere assorbiti da un



sistema di criminalità pedopornografica che ne sfrutta la ingenuità per ottenerne profitto, non solo personale.

I minori di qualunque età, nel momento in cui si avvicinano al mondo di Internet e alle sue infinite possibilità e occasioni, corrono il rischio, soprattutto, di finire vittime dei cosiddetti **Groomer**, pedofili che, al fine di adescare i ragazzi e avviare con essi relazioni sessuali, sfruttano il mondo con cui gli stessi interagiscono, utilizzandone qualsiasi spazio, modellando le proprie tecniche sulla base di ciò che, di volta in volta, risulti di tendenza. Il fenomeno ha assunto forme sempre differenti negli anni, sulla base degli sviluppi dell'informatica.

Non è raro, infatti, che si utilizzino delle app all'apparenza innocue per ottenere dai giovani utenti contenuti a sfondo sessuale, o appuntamenti offline: restando tale contatto all'interno di strumenti del tutto innocenti, spesso risulta molto difficoltoso per gli adulti anche solo venire a conoscenza di ciò che sta succedendo, peraltro essendo l'interazione con il web molto più discreta rispetto alla tradizionale "caramella dello sconosciuto".

Videogames con funzioni multiplayer online, app di messaggistica, social network: ogni occasione diventa preziosa per creare delle connessioni, giungendo dritti dritti nelle case delle vittime, costringendole spesso all'invio di immagini esplicite a fronte delle più disparate minacce.

È così che il materiale pedopornografico viene raccolto e successivamente diffuso all'interno di sistemi cloud o reti darknet gestiti secondo catene gerarchiche organizzate, quasi del tutto irrintracciabili ed anonimizzate, all'interno di quello che è **un vero e proprio business criminale** altamente redditizio e dalla difficile identificazione (nella loro accezione più estrema, capita anche che i servizi web siano utilizzati per l'organizzazione di reti di prostituzione minorile o di abusi "su prenotazione", per quei committenti che intendono pagare anche ingenti somme pur di accedere alla visione di suddetti contenuti illeciti).

Risultando impossibile difendere i propri piccoli di casa da ogni rischio che gli stessi possono incontrare sul web, **la tecnica migliore per proteggerli è quella di porre in essere una serie di**

comportamenti preventivi che possano consentire loro, sin dal primo momento in cui avvicinano ai servizi digitali, di **riconoscere tutte le situazioni di pericolo** e di percepire i "campanelli di allarme", non solo per proteggerne la privacy ma anche e soprattutto per tutelarne la libertà online.

Spiegare come gli hackers ottengano le passwords e altre informazioni aiuterà gli studenti a capire l'importanza di questa basilare abilità di sicurezza. Inoltre, gli studenti dovranno imparare a fronteggiare i Cyber bulli tramite esempi di vita reale per capire come agiscono. Questo è lo scopo del nostro progetto KA229 Erasmus+.