Internet: mondo virtuale, pericoli reali
Conoscenza uguale sicurezza

Un convegno che il Rotary Club Cuorgné e Canavese ha organizzato il 4 maggio 2016 a Cuorgnè, nell'Auditorium della Manifattura messo a disposizione dal Sindaco del Comune di Cuorgnè. Relatore della serata il Sostituto Commissario Emilio Gallo –della Polizia Postale e delle Comunicazioni.

Convegno reso possibile grazie alla collaborazione degli Istituti Scolastici del Canavese, del Consorzio Intercomunale dei Servizi Socio-Assistenziali C.I.S.S.38, dell'Associazione Ex Allievi di Rivarolo Canavese e del Rotaract Club Cuorgnè e Canavese.

Con patrocinio inoltre del Comune di Cuorgnè, del Comune di Agliè, del Comune di Castellamonte e del Comune di Rivarolo Canavese.

Tema e motivazione del convegno:

«Ormai siamo tutti connessi ad un mondo virtuale che diventa sempre più specchio del mondo reale ed in esso infine si riflette e si ripercuote. Il web apre grandi opportunità sociali ma può anche diventare veicolo per comportamenti scorretti, soprattutto tra i più giovani. Per questi ed altri motivi un incontro rivolto ai professori e ai genitori dei ragazzi delle scuole del territorio canavesano, per informarli sui rischi connessi ad un utilizzo superficiale della rete, non sempre consapevoli dei danni che possono arrecare e delle conseguenze a cui vanno incontro.»

Una carrellata fatta di deep web, cyberbullismo, spamming, social network, pedofilia on line, hacking, clonazione di mezzi pagamento, e-commerce per un uditorio attento e partecipativo.

In TV e sui giornali si sente parlare sempre più spesso di Deep Web, ma di cosa si tratta precisamente? Deep Web è una parte di Web "sommersa" in cui vengono svolte tantissime attività, da quelle più discutibili e illegali (come la vendita di documenti falsi) ad altre molto più "tranquille". Sono dunque dei siti "nascosti", che non si trovano facendo delle normali ricerche in Google e che possono essere visitati solo sfruttando accessi specialistici.

Cyberbulli: un'età compresa tra i 10 e i 16 anni, un'immagine di bravi studenti, una competenza informatica superiore alla media, incapacità a valutare la gravità delle azioni compiute on-line: questo l'identikit del cyber bullo, che usa internet per realizzare quello che magari non riesce a rivendicare nella vita reale, quello che non ha il coraggio di fare nel cortile della scuola

Spamming ovvero invio indiscriminato, senza il consenso del destinatario, di messaggi di posta elettronica. In concreto la casella di posta elettronica viene inondata da decine di e-mail, pubblicitarie e non, capaci di porre a rischio il funzionamento del servizio di posta elettronica della vittima. Un' etimologia particolare diventato sinonimo di fastidioso e non richiesto invio di valanga di materiale (e-mail).

I social network: siti come *Linkedin* , *Myspace*, *Instagram*, *Twitter*, o il più diffuso di tutti, *Facebook*, sono in grado di creare in brevissimo tempo relazioni ed interazioni tra migliaia di persone, trasformandoli in un importante veicolo anche per operazioni commerciali e di marketing; questo grazie alla circolazione e pubblicazione in tempo reale di giudizi, critiche, informazioni, immagini e video che per loro intrinseca natura possiedono una reale capacità di influenzare i gusti e le scelte degli utenti su prodotti e servizi offerti dai numerosissimi siti italiani ed esteri presenti sulla rete.

Pedofilia on-line, ovvero il comportamento di adulti pedofili che utilizzano la rete internet per incontrare altri pedofili (chat, forum, bbs), per alimentare le loro fantasie sessuali deviate, per rintracciare e scambiare materiale fotografico o video pedopornografici e per ottenere contatti o incontri con i bambini che sono sulla rete.

Hacking: hacker, qualcuno che ama esplorare le possibilità offerte da un sistema informativo e mettere alla prova le sue capacità, in contrapposizione con la maggior parte degli utenti che preferisce apprendere solo lo stretto indispensabile. Questo è, ovviamente, il concetto di hacker espresso con un valore positivo. Vi è tuttavia da segnalare che dell´intento puramente ludico che spingeva i primi hacker ad agire poco è rimasto. I sistemi informatici custodiscono, infatti, dati sempre più preziosi e la loro violazione arreca ormai danni notevoli ad aziende ed istituzioni pubbliche e governative. Da distinguere inoltre la figura dell´ hacker da quella del cracker. I cracker sono coloro che fanno attività di hacking a scopo di lucro. Entrambe le figure, per la legge italiana, sono punibili.

Il recente, esponenziale incremento dell'utilizzo dei mezzi di pagamento elettronico (bancomat e carte di credito/debito) ha richiamato l'attenzione delle organizzazioni criminali sia in relazione alla semplicità delle tecniche utilizzate sia in relazione ai notevoli profitti che tali attività consentono. I malviventi registrano i dati acquisiti dalle carte di pagamento dall'ignaro utente e contestualmente, tramite una microcamera nascosta o una tastiera sovrapposta, rilevano il PIN digitato. I dati così acquisiti consentiranno di creare carte clonate in grado di essere utilizzate per prelievi e transazioni illecite.

E-commerce: agli indubbi vantaggi che il commercio elettronico porta alle imprese ed ai consumatori, si accompagnano, tuttavia, nuove sfide e nuovi rischi per chi compra e per chi vende, dovuti anche alle dimensioni globali del fenomeno. C´è la necessità di creare fiducia e confidenza tra le parti in gioco, soprattutto per quanto riguarda l´identità dei soggetti, l´individuazione della sede del fornitore, l´integrità e la sicurezza dei messaggi scambiati, la protezione dei dati personali, la validità e l´efficacia del contratto stipulato per via telematica o informatica, la sicurezza nei pagamenti.