Conviviale 26 gennaio 2015
"**Navigare nella rete: consigli per non perdere la rotta**"
relatrice dott.ssa **Paola Capozzi**

La dott.ssa Paola Capozzi, in Polizia dal 1986, è stata una delle prime donne dirigenti della Polizia di Stato. Ha lavorato per otto anni ad Ivrea, per poi essere trasferita a Genova e poi nuovamente a Torino, dove è stata chiamata nel 2010 a ricoprire la carica di Responsabile I Dirigente della Polizia Postale e delle Comunicazioni per l'area Piemonte - Valle d'Aosta e, ultima aggiunta, Liguria.

Socia del nostro Club durante la sua permanenza a Ivrea, si è spostata al Club di Genova per poi ritornare da noi con il suo rientro a Torino.

Ce la ricordiamo tutte come una donna che si distingue per la Sua alta professionalità, ma anche per la Sua grande umanità, che la porta non solo a dare un tocco diverso al suo lavoro, ma a prendersi carico personalmente delle varie problematiche, a prevederne le conseguenze e ad anticiparle, trasferendo in maniera vivace e professionale tutto il Suo entusiasmo a chi ha la fortuna di lavorare con Lei.

La dott.ssa Capozzi con la relazione dal titolo: "Navigando nella rete: consigli per non perdere la rotta" ci ha guidati nel mondo di internet per farci capire non i vantaggi, che sono ovvii a tutti, ma come difenderci dai pericoli.

Non ne possiamo fare più a meno, poiché ormai la nostra civiltà si muove con esso, permettendoci di acquisire informazioni da tutto il pianeta, aumentando la nostra conoscenza personale con scambi di opinioni e punti di vista diversi, ad una velocità una volta impensabile.

Tuttavia, come in tutte le cose, ci sono gli aspetti positivi e quelli negativi. La velocità che ci permette di passare alla visione di un sito e poi ad un altro, per non parlare della vastità del mercato, che ci mette a disposizione l'acquisto di qualunque cosa, ci porta a sottovalutare la scelta di cosa compriamo e da chi lo compriamo.

La Polizia di Stato italiana è molto attenta ai pericoli cui siamo esposti e ha creato un sistema di difesa, invidiato a livello mondiale, al punto che l'F.B.I. ha mandato in Italia personale perché venisse formato sulle attività sia di prevenzione che di investigativa. Si tratta infatti di riuscire a coniugare le nuove tecniche con le più vecchie tecniche investigative di cui la Polizia italiana è sempre stata all'avanguardia.

Le slides che ci fa vedere Paola sono relative a tutto il lavoro che i 20 compartimenti e le 80 sezioni di Polizia Postale d'Italia stanno facendo per combattere il cosiddetto "cyber crime" cioè un crimine come tutti gli altri per obbiettivi e soggetti coinvolti, ma che si distingue per l'aggiunta dell'informatica, che ne diventa mezzo ed obbiettivo nello stesso tempo.

Questo tipo di crimine, che occupa il 50% dell'insieme dei rischi globali ed ha un fatturato di 10 miliardi di dollari all'anno (superiore a quello della droga) utilizza l'informatica per colpire obbiettivi informatici (computer, smartphone, iphone) e, attraverso di essi aziende, società, figure istituzionali, VIP e noi, semplici cittadini.

Non è un crimine facile da combattere per diversi motivi. La minaccia creata è aumentata del 254% negli ultimi anni e i danni sono aumentati con la sofisticazione delle tecniche informatiche.

E' un tipo di crimine che non ha confini fisici né di frontiere, né di legislatura. Infatti, mentre in Italia lo Stato ha creato delle norme che permettono di arrivare alla fonte, in altri stati, come la vasta ex Unione Sovietica o la Nigeria, le fonti sono tutelate e per tanto non possono essere bloccate.

E' in questi paesi che vengono piazzate le cosiddette " Centrali Master", che attraverso un gioco di rimando che parte da loro, ma che utilizzando i nostri computer ignari, si allarga ad effetto catena di San Pietro (bot net), bombardando di dati, contemporaneamente e in maniera massiccia, centrali informatiche di grosse aziende, fino a portarle al blocco.

Questo tipo di rischi ha portato a creare, da parte della Polizia, una centrale operativa che, attraverso un monitoraggio costante, permette di dare appoggio, in caso di un attacco, alle società rese vulnerabili.

Nelle nostre piccole realtà riescono ad infilarsi tramite il computer o lo smartphone, carpendo in formazioni su di noi e su quelli con cui comunichiamo, per quello che compriamo, per i nostri interessi personali e attraverso le chat e facebook, conoscono le nostre conversazioni. Quando facciamo una foto e la mettiamo in rete, tramite la geolocalizzazione comunichiamo dove siamo e ci sovraesponiamo. I giovanissimi sono sicuramente i più sovraesposti.

Da una slides ci siamo rese conto di come in fondo, quello di cui siamo a conoscenza è la punta di un iceberg, di come noi viaggiamo su una bella nave, che si potrebbe chiamare Google, ignari che sotto di noi ci sono sottomarini spia e mine, dislocati alle profondità più impensate, che ci fanno compagnia: il deep web.

L'unica maniera per proteggerci è prevenire e cioè essere informati dei rischi, poiché raggiungere i sommergibili è veramente difficile, per tutti i motivi detti prima.

Dobbiamo essere consapevoli che tutto ciò che viene messo in rete non si cancella più e che può essere usato contro di noi. Ci sono individui che utilizzano in nostri dati per farsi passare per altri e danneggiare altre persone ancora.

In Italia ci sono circa 27 miliardi di movimenti on line. Di questi più dell'80% è tramite computer e circa il 28% tramite smartphone, ma solo il 2% è consapevole del rischio a cui è esposto. In compenso siamo i primi in Europa, come istituzione, ad aver consapevolezza dei rischi dell'ackeraggio e del cyber crime.

Come possiamo difenderci? Evitando di far entrare chi vuole carpirci informazioni dentro il nostro computer & c.

E' un po' come nella favola di Cappuccetto Rosso e dei Sette Capretti: sapere con chi si ha a che fare e non aprire agli sconosciuti.

Tra le varie tecniche usate per colpirci ci sono i Malware (lett. Programma malvagio) virus che carpiscono informazioni, poi il Ransomware, programma che con un virus blocca il computer e dopo il pagamento di un riscatto, "in teoria", viene sbloccato. Fake quando qualcuno si finge di essere qualcun altro per carpirti informazioni. Il cosiddetto Fhishing che è una vera e propria banca di informazioni che studia, con indagini a largo spettro, le abitudini delle vittime per trovare il loro punto debole. A tal proposito c'è stata la visione di un video belga, dove si vede un uomo che facendosi passare per mago, racconta ad alcune persone aspetti della loro vita privata molto particolari, quasi segreti, rendendole sconcertate. Lo sono diventate ancora di più quando, caduto un telo dello sfondo, hanno visto un mega schermo con le loro foto che credevano private, gli

estratti delle loro spese e le conversazioni con i loro amici ed un gruppo di persone che smanettava su computer.

Bisogna tenere aggiornati gli antivirus e purtroppo quelli gratuiti non sono sinonimo di garanzia, anzi. Non aprire assolutamente le SPAM, anzi cestinarle immediatamente e non aprire e-mail di sconosciuti o di proposte attraenti che vanno dalla vacanza alla vincita di qualunque cosa.

Quando apriamo un sito o siamo su facebook controllare che l'URL (cioè la barra in alto) abbia veramente il nome di quello che stiamo cercando, perché potrebbe essere un altro, che fa da filtro in maniera parassita, e negli acquisti controllare che ci sia il lucchetto in alto a destra, perché è sinonimo di garanzia. Mai dare informazioni sulla nostra carta di credito anche se richiesto dalla Visa e utilizzare carte prepagate.

Un ultimo capitolo è da dedicare, purtroppo alla pedofilia on line. I pedofili non sono facili da stanare poiché, benchè ogni computer abbia un suo numero di matricola, si muovono attraverso canali depistatori, che non permettono di risalire direttamente a loro. Hanno un linguaggio ed una metodologia di approccio che incanta il minore ed è per questo che bisogna controllare costantemente cosa fanno i nostri figli al computer, guardando in prima persona.

La Polizia ha creato il CNCPO, una task force che tratta la pedofilia alla stessa stregua del terrorismo e la legislazione ha permesso la formazione di personale che, sotto copertura, è in grado di fingersi a sua volta pedofilo, nel tentativo di avvicinarsi il più possibile alla fonte.

Posso dire che nessuna di noi si è annoiata ascoltando questa relazione, anzi, ne siamo uscite un po' sgomente, ma anche confortate da tutto quello che si sta facendo per proteggerci, grazie a persone che ci mettono l'anima come Paola Capozzi ed i suoi colleghi. Da parte nostra, come solo noi donne sappiamo fare, cercheremo di far girare il più possibile tutto quello che abbiamo imparato per evitare di essere utilizzate, a nostra insaputa, da loschi personaggi con obbiettivi tutt'altro che benefici.