Navigare sicuri in rete

Obbiettivo: *conoscenza delle minacce informatiche al fine di evitarne il contagio e saperle riconoscere.*

Risorse: *consultazione di un esperto del settore informatico.*

Internet, al giorno d'oggi, è una delle più potenti risorse al mondo.
Ci permette di spedire: file, posta, immagini e svolgere moltissime altre cose di uso quotidiano e personale in tempi brevissimi.
Il giorno 21/03/2015, grazie ad un progetto scolastico, siamo riusciti ad avere la consulenza di un esperto del settore informatico, che ci ha spiegato in modo semplice ed elementare quali sono le più imponenti minacce per una risorsa così potente. Ebbene sì, come ogni cosa costruita dall'uomo, anche internet ha dei lati negativi. Per iniziare, l'esperto ci ha spiegato partendo da come la corretta collocazione del nostro pc (ma anche telefono, tablet e altri) sia importante poiché deve necessariamente essere in un ambiente idoneo, non troppo caldo, né troppo freddo, posizionato su un piano stabile per prevenire ribaltamenti e/o rotture del nostro apparecchio. Ha proseguito con le protezioni così dette *"attive",* che permettono a livello software di prevenire una perdita completa dei dati. Una delle più comuni protezioni che ogni dispositivo dovrebbe necessariamente avere è un buon antivirus, ovvero un programma la cui funzione è di evitare di far entrare in contatto il nostro pc con software creati da terzi con l'intenzione di danneggiarlo. Un altro programma, che non tutti sanno cos'è, è il *firewall*: un programma pre-installato all'interno del computer, che monitora costantemente le relazioni del dispositivo verso la rete, o per meglio dire verso l'esterno. Come accennavo prima, esistono anche malintenzionati (esperti del settore), che hanno lo scopo di "rubare" dati privati che noi tutti

abbiamo all'interno delle nostre apparecchiature; per farlo sfruttano programmi creati da loro stessi, detti ***malware***, ovvero software dannosi; molto spesso sono utilizzati a livello aziendale per fornire alle società informazioni per scopi di marketing. I malware più comuni sono quelli che sono capaci di individuare ogni lettera digitata, ma anche quelli che riescono a "comandare" tramite remoto (da casa dell'aggressore) il nostro pc, anche se fisicamente sono in due posizioni diverse.
Dopo una buona spiegazione generale sui malware, l'esperto ha introdotto poi il termine *"virus"*. E' chiamato in questo modo perché ha la principale caratteristica di un virus biologico, ovvero la capacità di replicarsi. Infatti, a livello informatico, un virus è un programma che, una volta avviato (anche in modo non visibile), comincia la riproduzione facendo copie di se stesso, comportando così: rallentamento generale del dispositivo, riempimento del disco fisso per l'archiviazione dei dati, impossibilità o arresto improvviso di programmi che potrebbero fermare il virus stesso, nuovi nomi a molteplici file, cancellazione dei file stessi. Un virus può non soltanto essere "fastidioso", ma può addirittura manomettere il corretto funzionamento della tastiera.
Lo specialista ci ha spiegato più nel dettaglio, quali sono i pericoli più comuni e dannosi: worm, pishing, cryptolocker.

I ***"Worm"***: sono di solito allegati che possiamo trovare nelle diffusissime mail, usate frequentemente nel mondo del lavoro. Questi piccoli allegati non hanno bisogno di essere eseguiti, ma una volta attivati automaticamente non fanno altro che replicarsi e recare danni al dispositivo.

Il ***"Pishing"***: tecnicamente parlando non è un virus, ma più che altro è un metodo di adescamento dei malcapitati da parte di malintenzionati. Esso consiste nel creare un sito fittizio che a livello grafico è identico al sito originale, per cui le credenziali che si inseriranno per tentare l'accesso non andranno al sito originale, ma verranno mandate ai proprietari del sito fittizio, che poi potranno utilizzarle come vorranno.

I ***"Cryptolocker"***: sono file di tipo eseguibile che una volta avviati sono molto difficili da eliminare, poiché il loro funzionamento è quello di prendere ogni file e criptarlo. La criptazione è risolvibile sole se si è a conoscenza della chiave, meglio conosciuta come "password", o dell'algoritmo utilizzato per la criptazione. L'intento di questo virus non è quello del danneggiamento, ma di ottenere un riscatto.

Un modo efficace per evitare tutte queste minacce (ci consiglia sarcasticamente l'esperto) è quello di spegnere il pc.
Ma ci dice anche, con la sua esperienza, che il modo migliore è quello di creare periodicamente dei ***"backup"***, ovvero copie per il ripristino completo del dispositivo (in fase sicura) che potranno essere eseguite nei momenti nei quali il dispositivo è infetto.

FRANCESCO PIERSANTI (2°G)

ITIS "ALESSANDRINI"